KeyFinder By Luigi Origa

Edit by Raoul Origa

Command List

```
Key Finder by Luigi Origa [V1.0 May 20 2024-00:15:47]
-h                                this help
-i path|filename                  path or binary to load
-th number                        number of threads
-x                                extract certificate x509
-r                                scan recursive directory
+-ed25519 ed448 secp256k1         enable/disable algorithm
-no_cross                         disable cross scan
-certs_only                       search for certificates only
```

Key search on a single file

```
C:\Progetti\btc_pubkeys\KeyFinder\Win64\Release>KeyFinder.exe  -i C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin
Key Finder by Luigi Origa [V1.0 May 26 2024-10:51:24]
Add C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin
Found 1 files to check
Using: 4 threads
ED25519: enabled
ED448: enabled
Cross Search: enabled
Load C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin
Loading <C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin>
Hashing buffer...
Hashing 3092
Thread exit...OK
Created 12773 unique keys
Saving...C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin.P32
Saved 12773 keys
Creating ED25519 pubkey...
4152/sec 11238 12773 elapsed ~3s remaining ~0s
Saving...C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin.KED255192
Saved 12773 keys
Search pubkeys...
FOUND ED25519 priv:1498b5467a63dffa2dc9d9e069caf075d16fc33fdd4c3b01bfadae6433767d93 pub:b7a3c12dc0c8c748ab07525b701122b88bd78f600c76342d27f25e5f92444cde
FOUND ED25519 priv:0305334e381af78f141cb666f6199f57bc3495335a256a95bd2a55bf546663f6 pub:dfc9425e4f968f7f0c29f0259cf5f9aed6851c2bb4ad8bfb860cfee0ab248292
FOUND ED25519 priv:833fe62409237b9d62ec77587520911e9a759cec1d19755b7da901b96dca3d42 pub:ec172b93ad5e563bf4932c70e1245034c35467ef2efd4d64ebf819683467e2bf
Load C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin
Loading <C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin>
Hashing buffer...
98/100
Thread exit...OK
Created 7463 unique keys
Saving...C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin.P57
Saved 7463 keys
Creating ED448 pubkey...
1688/sec 5788 7463 elapsed ~7s remaining ~0s
Saving...C:\Progetti\btc_pubkeys\KeyFinder\TEST\test.bin.KED448
Saved 7463 keys
Search pubkeys...
FOUND ED448 priv:c4eab05d357007c632f3dbb48489924d552b08fe0c353a0d4a1f00acda2c463afbea67c5e8d2877c5e3bc397a659949ef8021e954e0a12274e pub:43ba28f430cdff456ae531545f7ecd0ac834a55d9358c0372bfa0c6c
6798c0866aea01eb00742802b8438ea4cb82169c235160627b4c3a9480
FOUND ED448 priv:6c82a562cb808d10d632be89c8513ebf6c929f34ddfa8c9f63c9960ef6e348a3528c8a3fcc2f044e39a3fc5b94492f8f032e7549a20098f95b pub:5fd7449b59b461fd2ce787ec616ad46a1da1342485a70e1f8a0ea75d
80e96778edf124769b46c7061bd6783df1e50f6cd1fa1abeafe8256180
FOUND ED448 priv:5bf99800a249752e038f2f49945bfca3394e042fcc3f8a8c52a348e3f60e96c9639f8cfadd349f926cbf3e51c889be32d6108d80cb62a5826c pub:b90c5d6bd882b2490b7469b810b95b44fa7a0ae9aaaaca4b6b49b069
e70eff67d7627b525a398063633092b392ec6a819e5e927834f3f16a80
FOUND ED448 priv:1289f6ad707e1affcdf232c77083e501ce79840a63c35d1dc95f68dbe1544cfee280ebb1f9fa4549b6f2353e3039b2a08f5c7cded0dadd927c pub:5d9814ea9fa163dd4152ac50296d6e1e0a64af1539bc4b04bbb42d8a
771674256535d74eca5277aeee0d169f5dcf08879e4e5f4e0c329f2d80
*** CROSS COMPARE **
Done! Bye

C:\Progetti\btc_pubkeys\KeyFinder\Win64\Release>
```

Cross Key search ED25519

```
C:\Progetti\btc_pubkeys\KeyFinder\Win64\Release>KeyFinder.exe -i z:\d\xx\certs_ed25519\ -r
Key Finder by Luigi Origa [V1.0 May 26 2024-10:51:24]
Scanning z:\d\xx\certs_ed25519\
Found 12 files to check
Using: 4 threads
ED25519: enabled
ED448: enabled
Cross Search: enabled
Load z:\d\xx\certs_ed25519\private\key_1.der
Loading <z:\d\xx\certs_ed25519\private\key_1.der>
Hashing buffer...
17/100
Thread exit...OK
Created 68 unique keys
```

```
Search pubkeys...
*** CROSS COMPARE **
FOUND ED25519 z:\d\xx\certs_ed25519\private\key_1.der priv:8b7528c44e7f1aaf1d4df2f6c3af8eb1ec9324c4bfc1cbad3717afceb73ca1c6 z:\d\xx\certs_ed25519\public\key_1.der pub:21028bbbb83a8df0777ac66c87236a89b7532314a2034ad957ed7c03d70186bf
FOUND ED25519 z:\d\xx\certs_ed25519\private\key_2.der priv:dfcb102b5cd11d9fd8544e55289d2c15de1862278a851d6411f56ad8d9cb06e8 z:\d\xx\certs_ed25519\public\key_2.der pub:200d784f31bfa0fba66c49a1eb666fec44749b52c5d1ec3febe0ce6372a1c5cf
FOUND ED25519 z:\d\xx\certs_ed25519\private\key_3.der priv:197b14556006013026ec31a964ac7bbe97e292773e066318c2d7bc6019603310 z:\d\xx\certs_ed25519\public\key_3.der pub:ac34ba2e015f0b512ea19d4ec121beb73c015c2840d3e864e9422b87e8456401
Error: z:\d\xx\certs_ed25519\private\key_1.der.KED448 not found
Done! Bye
```

Cross Key search ED448

```
C:\Progetti\btc_pubkeys\KeyFinder\Win64\Release>KeyFinder.exe -i z:\d\xx\certs_ed448\*.der -r
Key Finder by Luigi Origa [V1.0 May 26 2024-10:51:24]
Scanning z:\d\xx\certs_ed448\*.der
Found 6 files to check
Using: 4 threads
ED25519: enabled
ED448: enabled
Cross Search: enabled
Load z:\d\xx\certs_ed448\public\key_3.der
```

```
Creating ED448 pubkey...
7/sec 7 26 elapsed ~0s remaining ~2s
Saving...z:\d\xx\certs_ed448\public\key_2.der.KED448
Saved 26 keys
Search pubkeys...
*** CROSS COMPARE **
FOUND ED448 z:\d\xx\certs_ed448\private\key_3.der priv:a2704ddfbcd590bce56e524f835c7890490df8f3e510d85165735010b36033cce60223fa0fb6f1cbcc65546971e5b8e6243cbdd3d36abee830 z:\d\xx\certs_ed448\public\key_3.der pub:bf0145db66e544d744f9397e49dc47b58ec32fedcc884e7b7dff5e7880a43714feeb0e444821b416615667dc5daf61439214bba674ad057880
FOUND ED448 z:\d\xx\certs_ed448\private\key_1.der priv:6e59ad89708bde32b4c599bee7fa26b3ea38219cbdd2d02fbe77d8d9949e6c809beec293b8e58d2da3bb005944558e85b6721465871369030f z:\d\xx\certs_ed448\public\key_1.der pub:71bccf94dff0634517c3e3be8fa8dfdbd427589c6c56b3c3c73cfb5cdf8b775d0a52e4b00f078b249c2ec635511eb30b601b7a93ba59906f80
FOUND ED448 z:\d\xx\certs_ed448\private\key_2.der priv:c59293c97b1f9fa07aabe0ee8ecfa26c52049eb97ad076bdac61766893ee7514cdd86f002e0dd9c5a0b796a374a628fa781d622e884eeec0b0 z:\d\xx\certs_ed448\public\key_2.der pub:764cc66652cf8c8337b538296bf7a8cd6431916d68eb95a2c6153a29ddc1f72ac30294beed5ff6597cc6976f5b5dd556587979a2ba80b7b600
Done! Bye
```

Script for creating test files

```
#!/bin/bash

CURVE=ed25519

rm certs_$CURVE -r

mkdir certs_$CURVE
mkdir certs_$CURVE/private
mkdir certs_$CURVE/public

for ((i=1; i<=$1; i++))
do
        openssl genpkey -algorithm ed25519 -outform PEM -out certs_$CURVE/private/key_$i.pem
        openssl pkey -in certs_$CURVE/private/key_$i.pem -pubout -outform PEM -out certs_$CURVE/public/key_$i.pem
        openssl pkey -inform PEM -outform DER -in certs_$CURVE/private/key_$i.pem -out certs_$CURVE/private/key_$i.der
        openssl pkey -pubin -inform PEM -outform DER -in certs_$CURVE/public/key_$i.pem -out certs_$CURVE/public/key_$i.der
done

echo "done!"
```

```
#!/bin/bash

CURVE=ed448

rm certs_$CURVE -r

mkdir certs_$CURVE
mkdir certs_$CURVE/private
mkdir certs_$CURVE/public

for ((i=1; i<=$1; i++))
do
    openssl genpkey -algorithm ed448 -outform PEM -out certs_$CURVE/private/key_$i.pem
    openssl pkey -in certs_$CURVE/private/key_$i.pem -pubout -outform PEM -out certs_$CURVE/public/key_$i.pem
    openssl pkey -inform PEM -outform DER -in certs_$CURVE/private/key_$i.pem -out certs_$CURVE/private/key_$i.der
    openssl pkey -pubin -inform PEM -outform DER -in certs_$CURVE/public/key_$i.pem -out certs_$CURVE/public/key_$i.der
done

echo "done!"
```

Test files for ED25519 and ED448

```
kikkus@ubuntu:/mnt/hgfs/D/xx$ ./cert_ed25519 3
rm: cannot remove 'certs_ed25519': No such file or directory
done!
kikkus@ubuntu:/mnt/hgfs/D/xx$ ./cert_ed448 3
rm: cannot remove 'certs_ed448': No such file or directory
done!
kikkus@ubuntu:/mnt/hgfs/D/xx$ ls certs_ed25519/
private  public
kikkus@ubuntu:/mnt/hgfs/D/xx$ ls certs_ed25519/private/
key_1.der  key_1.pem  key_2.der  key_2.pem  key_3.der  key_3.pem
kikkus@ubuntu:/mnt/hgfs/D/xx$ ls certs_ed25519/public/
key_1.der  key_1.pem  key_2.der  key_2.pem  key_3.der  key_3.pem
kikkus@ubuntu:/mnt/hgfs/D/xx$ ls certs_ed448/
private  public
kikkus@ubuntu:/mnt/hgfs/D/xx$ ls certs_ed448/private/
key_1.der  key_1.pem  key_2.der  key_2.pem  key_3.der  key_3.pem
kikkus@ubuntu:/mnt/hgfs/D/xx$ ls certs_ed448/public/
key_1.der  key_1.pem  key_2.der  key_2.pem  key_3.der  key_3.pem
```

Script for creating more test files

```
#!/bin/bash

PATH_CERTS=certs_rand
CD=$(pwd)

rm $PATH_CERTS -r

mkdir $PATH_CERTS

generate_random_data() {
        size=$((RANDOM % 1024))
        head -c "$size" /dev/urandom
}

for ((i=1; i<=$1; i++))
do
        generate_random_data >> $PATH_CERTS/cert_$i.bin

    openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:secp256k1 -outform PEM -out /tmp/secp256k1_private_key_$i.pem
    openssl ec -pubout -in /tmp/secp256k1_private_key_$i.pem -outform PEM -out /tmp/secp256k1_public_key_$i.pem
    openssl pkey -inform PEM -outform DER -in /tmp/secp256k1_private_key_$i.pem -out /tmp/secp256k1_private_key_$i.der
    openssl pkey -pubin -inform PEM -outform DER -in /tmp/secp256k1_public_key_$i.pem -out /tmp/secp256k1_public_key_$i.der

        echo "** SECP256K1 PUB **" >> $PATH_CERTS/cert_$i.bin
        cat /tmp/secp256k1_public_key_$i.der >> $PATH_CERTS/cert_$i.bin

        generate_random_data >> $PATH_CERTS/cert_$i.bin

        echo "** SECP256K1 PRIV **" >> $PATH_CERTS/cert_$i.bin
        cat /tmp/secp256k1_private_key_$i.der >> $PATH_CERTS/cert_$i.bin

        generate_random_data >> $PATH_CERTS/cert_$i.bin

        openssl ecparam -name secp256k1 -genkey -noout -out /tmp/private_secp256k1.key
        openssl req -new -key /tmp/private_secp256k1.key -out /tmp/request_secp256k1.csr
        openssl x509 -req -days 365 -in /tmp/request_secp256k1.csr -signkey /tmp/private_secp256k1.key -out /tmp/certificate_secp256k1.crt
        openssl x509 -in /tmp/certificate_secp256k1.crt -outform der -out /tmp/certificate_secp256k1.der

        echo "** SECP256K1 CERT **" >> $PATH_CERTS/cert_$i.bin
        cat /tmp/certificate_secp256k1.der >> $PATH_CERTS/cert_$i.bin
        generate_random_data >> $PATH_CERTS/cert_$i.bin

        openssl genpkey -algorithm ed25519 -outform PEM -out /tmp/ed25519_private_key_$i.pem
        openssl pkey -in /tmp/ed25519_private_key_$i.pem -pubout -outform PEM -out /tmp/ed25519_public_key_$i.pem
        openssl pkey -inform PEM -outform DER -in /tmp/ed25519_private_key_$i.pem -out /tmp/ed25519_private_key_$i.der
        openssl pkey -pubin -inform PEM -outform DER -in /tmp/ed25519_public_key_$i.pem -out /tmp/ed25519_public_key_$i.der

        echo "** ED25519 PUB **" >> $PATH_CERTS/cert_$i.bin
        cat /tmp/ed25519_public_key_$i.der >> $PATH_CERTS/cert_$i.bin

        generate_random_data >> $PATH_CERTS/cert_$i.bin
```

Script for creating more test files

```
kikkus@ubuntu:/mnt/hgfs/D/xx$ ./cert_rand
rm: cannot remove 'certs_rand': No such file or directory
./cert_rand: line 15: ((: i<=: syntax error: operand expected (error token is "<=")
done!
kikkus@ubuntu:/mnt/hgfs/D/xx$ ./cert_rand 3
read EC key
writing EC key
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Signature ok
subject=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
Getting Private key
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

```
echo "done!"
kikkus@ubuntu:/mnt/hgfs/D/xx$ ls certs_
certs_ed25519/ certs_ed448/   certs_rand/
kikkus@ubuntu:/mnt/hgfs/D/xx$ ls certs_rand/
```

Key search on test files

```
C:\Progetti\btc_pubkeys\KeyFinder\Win64\Release>KeyFinder.exe -i z:\d\xx\certs_rand\*.*
Key Finder by Luigi Origa [V1.0 May 26 2024-10:51:24]
Scanning z:\d\xx\certs_rand\*.*
Found 3 files to check
Using: 4 threads
ED25519: enabled
ED448: enabled
Cross Search: enabled
Load z:\d\xx\certs_rand\cert_1.bin
Loading <z:\d\xx\certs_rand\cert_1.bin>
Hashing buffer...
Hashing 3017
Thread exit...OK
Created 29404 unique keys
Saving...z:\d\xx\certs_rand\cert_1.bin.P32
Saved 29404 keys
Creating ED25519 pubkey...
4543/sec 23809 29404 elapsed ~5s remaining ~1s
Saving...z:\d\xx\certs_rand\cert_1.bin.KED255192
Saved 29404 keys
Search pubkeys...
FOUND ED25519 priv:586f7fddd9c5cc869cf9ad4a81462a91a3f764e6ba12aa6e28b3a727a3259b86 pub:117fee1e5dcd32c78e273ade2badbb9321fafe83b5ac4c20248a0cd15598f79c
Load z:\d\xx\certs_rand\cert_1.bin
Loading <z:\d\xx\certs_rand\cert_1.bin>
Hashing buffer...
Hashing 742
Thread exit...OK
Created 14952 unique keys
Saving...z:\d\xx\certs_rand\cert_1.bin.P57
Saved 14952 keys
Creating ED448 pubkey...
1853/sec 14037 14952 elapsed ~17s remaining ~0s
Saving...z:\d\xx\certs_rand\cert_1.bin.KED448
Saved 14952 keys
Search pubkeys...
FOUND ED448 priv:80a1293dc47095f3b0d4d707943dc471f3729ae94503aa58bc910d321d862f03c1419dd984764044446e1099657c576c4cf26e6c4ecb1b5c128 pub:b77156f0147d1386e09202427103472081d3165ed1e7911d9c87a62650cc23d4e3e71a9394923ea2564117fa44b229d34f58767030d99b6200
Load z:\d\xx\certs_rand\cert_2.bin
Loading <z:\d\xx\certs_rand\cert_2.bin>
Hashing buffer...
Hashing 4528
Thread exit...OK
Created 23868 unique keys
Saving...z:\d\xx\certs_rand\cert_2.bin.P32
Saved 23868 keys
Creating ED25519 pubkey...
7899/sec 19598 23868 elapsed ~4s remaining ~0s
Saving...z:\d\xx\certs_rand\cert_2.bin.KED255192
Saved 23868 keys
Search pubkeys...
```

Certicate extraction

```
C:\Progetti\btc_pubkeys\KeyFinder\Win64\Release>KeyFinder.exe -i z:\d\xx\certs_rand\cert_3.bin -x
Key Finder by Luigi Origa [V1.0 May 26 2024-10:51:24]
Add z:\d\xx\certs_rand\cert_3.bin
Found 1 files to check
Using: 4 threads
ED25519: enabled
ED448: enabled
Cross Search: enabled
Loading <z:\d\xx\certs_rand\cert_3.bin>
Search and extract DER X509 certificate...
cert header found at 000007ea Size: 0x0000000000000186
cert header found at 00001027 Size: 0x0000000000000148
cert header found at 00001bce Size: 0x0000000000000194
Loading...z:\d\xx\certs_rand\cert_3.bin.KED255192
Trying to reserve memory for 30396 patterns... OK
Loaded 30396 keys
```

File analysis

```
C:\Progetti\btc_pubkeys\KeyFinder\Win64\Release>KeyFinder.exe -i "z:\d\xx\db504 v5.14 - Mqtt 12-07-2018.bin" -analyze
Key Finder by Luigi Origa [V1.0 May 26 2024-10:51:24]
Add z:\d\xx\db504 v5.14 - Mqtt 12-07-2018.bin
Found 1 files to check
Using: 4 threads
ED25519: enabled
ED448: enabled
Cross Search: enabled
Loading <z:\d\xx\db504 v5.14 - Mqtt 12-07-2018.bin>
```

Name	Score	Max	%
aes	1000	2750	36.36
sha256	20559	23308	88.21
sha512	0	26802	0.00
secp112r1	0	6000	0.00
secp112r2	0	5856	0.00
secp128r1	0	3936	0.00
secp128r2	0	4749	0.00
secp128r2	100	2873	3.48
secp160r1	0	3621	0.00
secp160r2	0	3773	0.00
secp192k1	83	2747	3.02
secp192r1	0	3665	0.00
secp224k1	0	2655	0.00
secp224r1	0	3570	0.00
secp256k1	62	2654	2.34
secp256r1	0	3684	0.00
secp384r1	0	3456	0.00
secp521r1	0	3255	0.00
brainpoolP160r1	0	5500	0.00
brainpoolP192r1	0	5664	0.00
brainpoolP224r1	0	5641	0.00
brainpoolP256r1	0	5435	0.00
brainpoolP256r1	0	5550	0.00
brainpoolP384r1	0	5706	0.00
brainpoolP512r1	0	5246	0.00
Curve22519	62	1810	3.43
Curve448	0	1479	0.00
Ed22519	62	1810	3.43
Ed448	0	1479	0.00
RSA Prime(8)	0	1000	0.00
RSA Prime(32)	0	254	0.00
RSA Prime	0	167	0.00

```
Load z:\d\xx\db504 v5.14 - Mqtt 12-07-2018.bin
```