? admin ??SSH????
$ su
This applet requires root priviledges!

??root
$vi /etc/passwd ?
root:TnU5p4RsVcJYk:0:0:root:/root:/bin/sh
nobody:*:500:499:Nobody:/var:/bin/nologin
admin:bmkVMsQ70yhfc:501:499:admin:/home:/bin/sh
(???? passwd??? admin??????)
TnU5p4RsVcJYk hash ????

??

http://support.ceci.com.tw/support/T...C%E6%AA%94.htm

http://blog.roodo.com/retsu0/archives/2642612.html

John the Ripper password cracker ???
http://www.openwall.com/john/g/john179j5w.zip ??

????? ? "TnU5p4RsVcJYk" ?? 1.TXT?
john-omp -i:all 1.txt
??john ????? hash ????

```
C:\Users\user>C:\Users\user\Desktop\run\john-omp.exe C:\Users\user\De
.txt
cygwin warning:
  MS-DOS style path detected: C:\Users\user\Desktop\run\1.txt
  Preferred POSIX equivalent is: /run/1.txt
  CYGWIN environment variable option "nodosfilewarning" turns off thi
  Consult the user's guide for more details about POSIX paths:
    http://cygwin.com/cygwin-ug-net/using.html#using-pathnames
Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
```
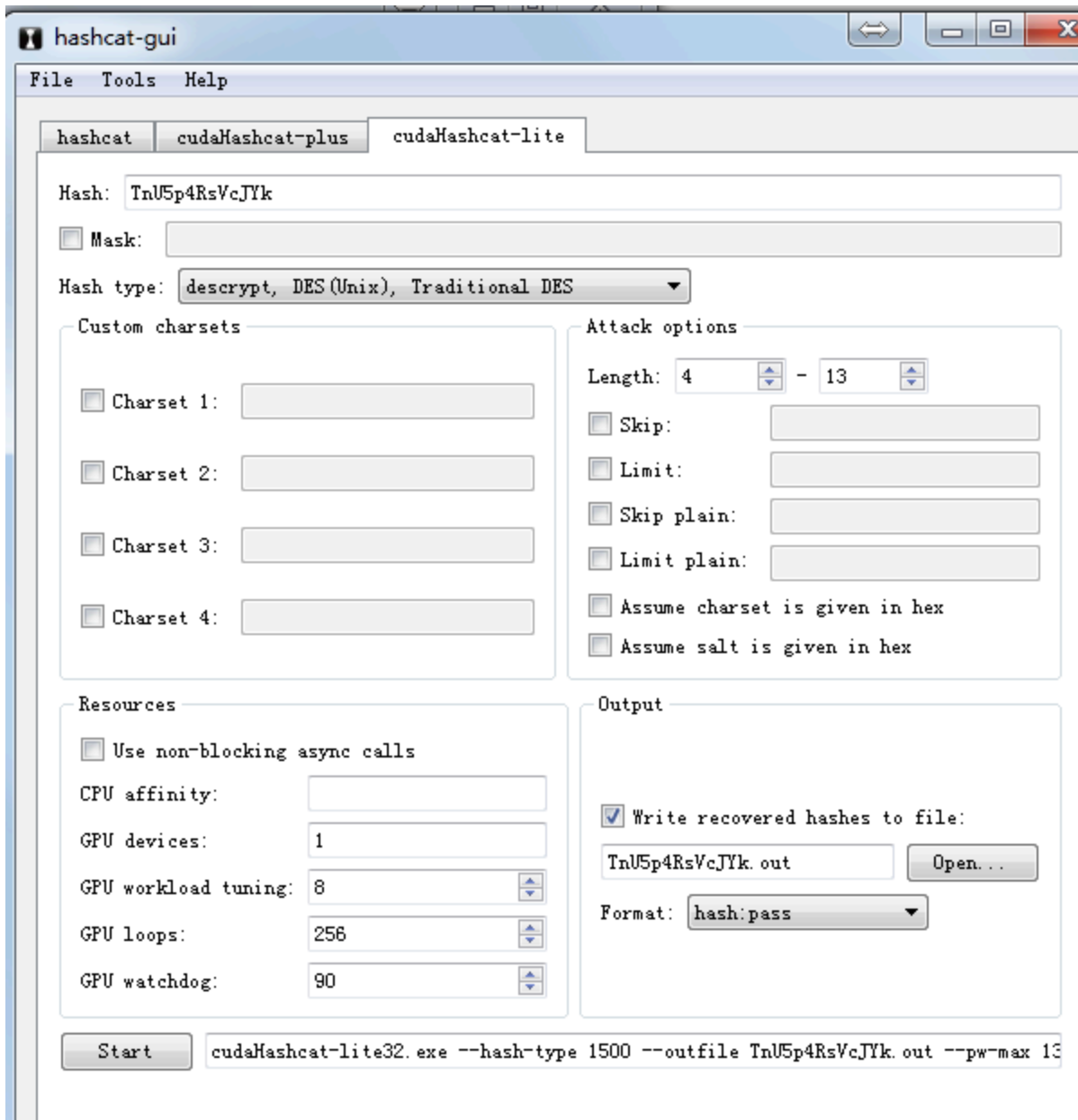
??? DES ????
John ????(i7-2600) ?? 3???? .
????hashcatlite

http://hashcat.net/hashcat-gui/ ????
??Nvidia GTX 570 ???
?????

```
hashcat-gui
File  Tools  Help

  hashcat   cudaHashcat-plus   cudaHashcat-lite

  Hash:  TnU5p4RsVcJYk

  ☐ Mask:

  Hash type:  descrypt, DES(Unix), Traditional DES   ▼

  ┌ Custom charsets ──────────────┐  ┌ Attack options ──────────────┐
  │                               │  │  Length:  4  ⬍  -  13  ⬍     │
  │   ☐ Charset 1:  [         ]   │  │  ☐ Skip:        [         ]  │
  │                               │  │                              │
  │   ☐ Charset 2:  [         ]   │  │  ☐ Limit:       [         ]  │
  │                               │  │                              │
  │   ☐ Charset 3:  [         ]   │  │  ☐ Skip plain:  [         ]  │
  │                               │  │  ☐ Limit plain: [         ]  │
  │   ☐ Charset 4:  [         ]   │  │  ☐ Assume charset is given in hex │
  │                               │  │  ☐ Assume salt is given in hex   │
  └───────────────────────────────┘  └──────────────────────────────┘

  ┌ Resources ────────────────────┐  ┌ Output ──────────────────────┐
  │  ☐ Use non-blocking async calls│  │                              │
  │  CPU affinity:   [         ]   │  │  ☑ Write recovered hashes to file: │
  │  GPU devices:    [1        ]   │  │  [TnU5p4RsVcJYk.out]  [Open...] │
  │  GPU workload tuning: [8   ]⬍  │  │  Format:  [hash:pass    ▼]    │
  │  GPU loops:      [256     ]⬍   │  │                              │
  │  GPU watchdog:   [90      ]⬍   │  │                              │
  └───────────────────────────────┘  └──────────────────────────────┘

  [ Start ]  cudaHashcat-lite32.exe --hash-type 1500 --outfile TnU5p4RsVcJYk.out --pw-max 13
```

```
Status.......: Cracked
Hash.Target..: TnU5p4RsVcJYk
Hash.Type....: descrypt, DES(Unix), Traditional DES
Time.Running.: 21 hours, 36 minutes
Time.Left....: 1 day, 21 hours
Plain.Mask...: ?1?2?2?2?2?2?2?3
Plain.Text...: ***aykin
Plain.Length.: 8
Progress.....: 1785790586880/5533380698112 (32.27%)
Speed.GPU.#1.: 23113.2k/s
HWMon.GPU.#1.:  0% GPU, 86c Temp
```

Nvidia GTX 570 ?????21 hours
root password = ntxadmin

?ip :ifconfig eth0 192.168.1.2