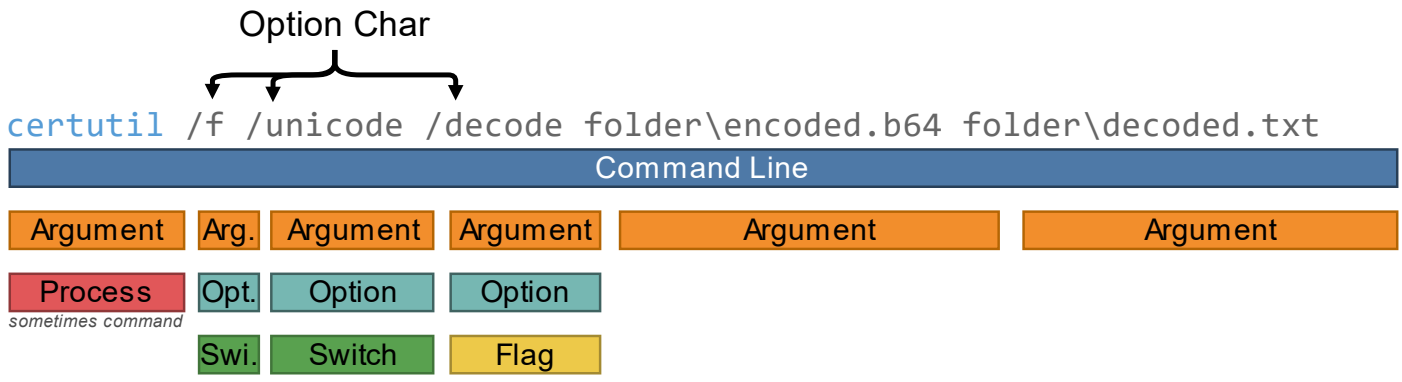

Option Char
certutil /f /unicode /decode folder\encoded.b64 folder\decoded.txt
Command Line
Argument
Arg.
Argument
Argument
Argument
Argument
Process
sometimes command
Opt.
Option
Option
Swi.
Switch
Flag

`/` `-`

`ping`

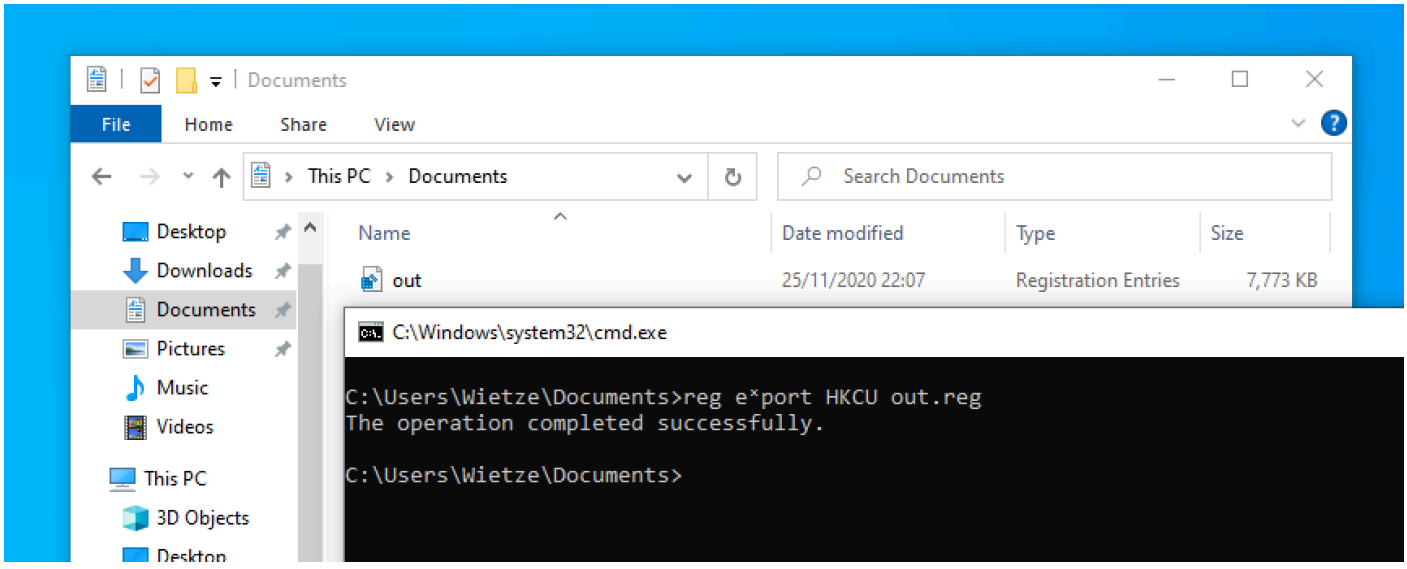
`ping -n 0 127.0.0.1`

`ping /n 0 127.0.0.1`

`find /i keyword`
`find -i keyword`

`certutil`

`reg` `reg export HKCU out.reg` `reg e^port HKCU out.reg`

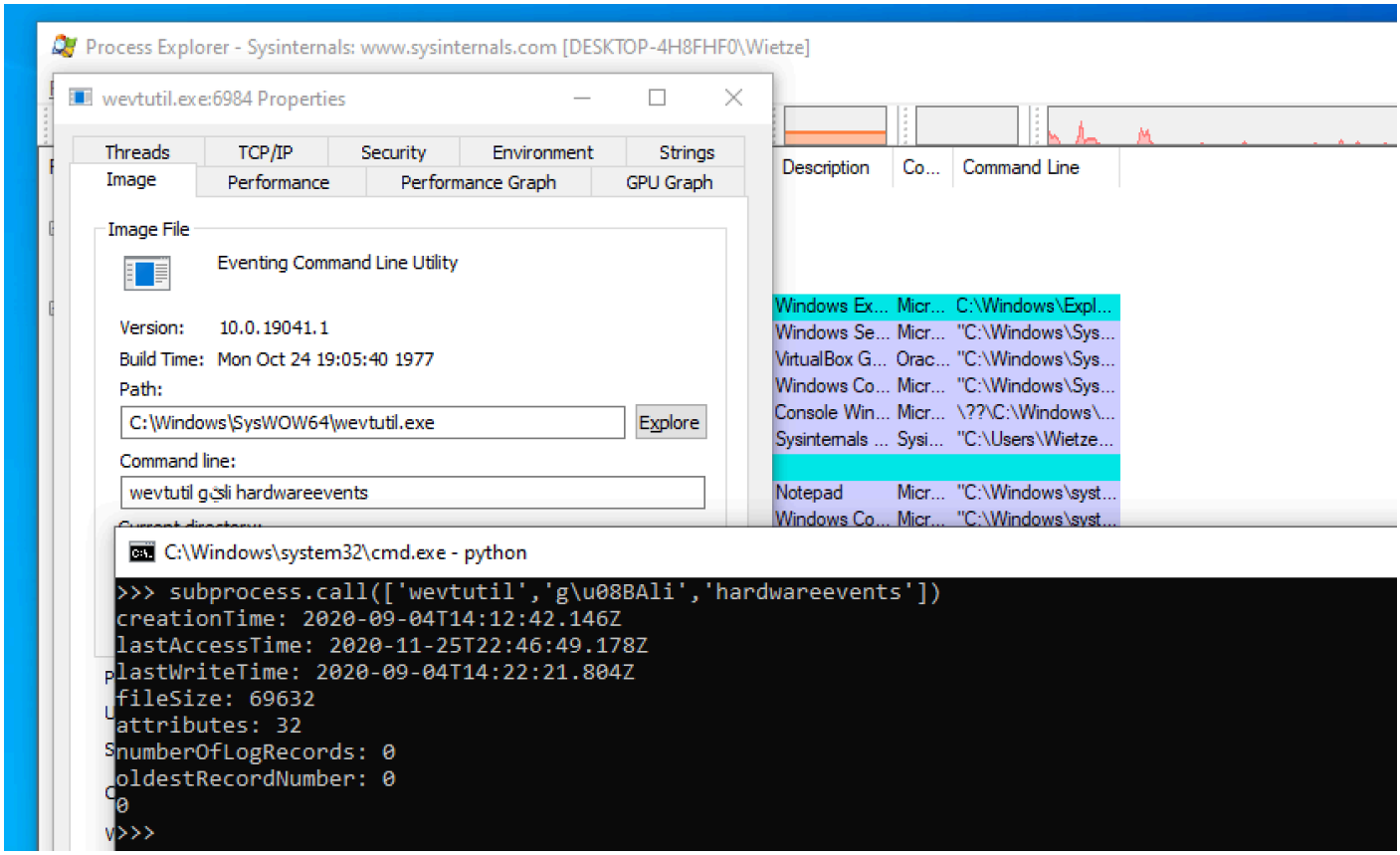


`reg e^port HKCU out.reg`

`wevtutil`

`wevtutil gli hardwareevents`

`wevtutil gچli hardwareevents`

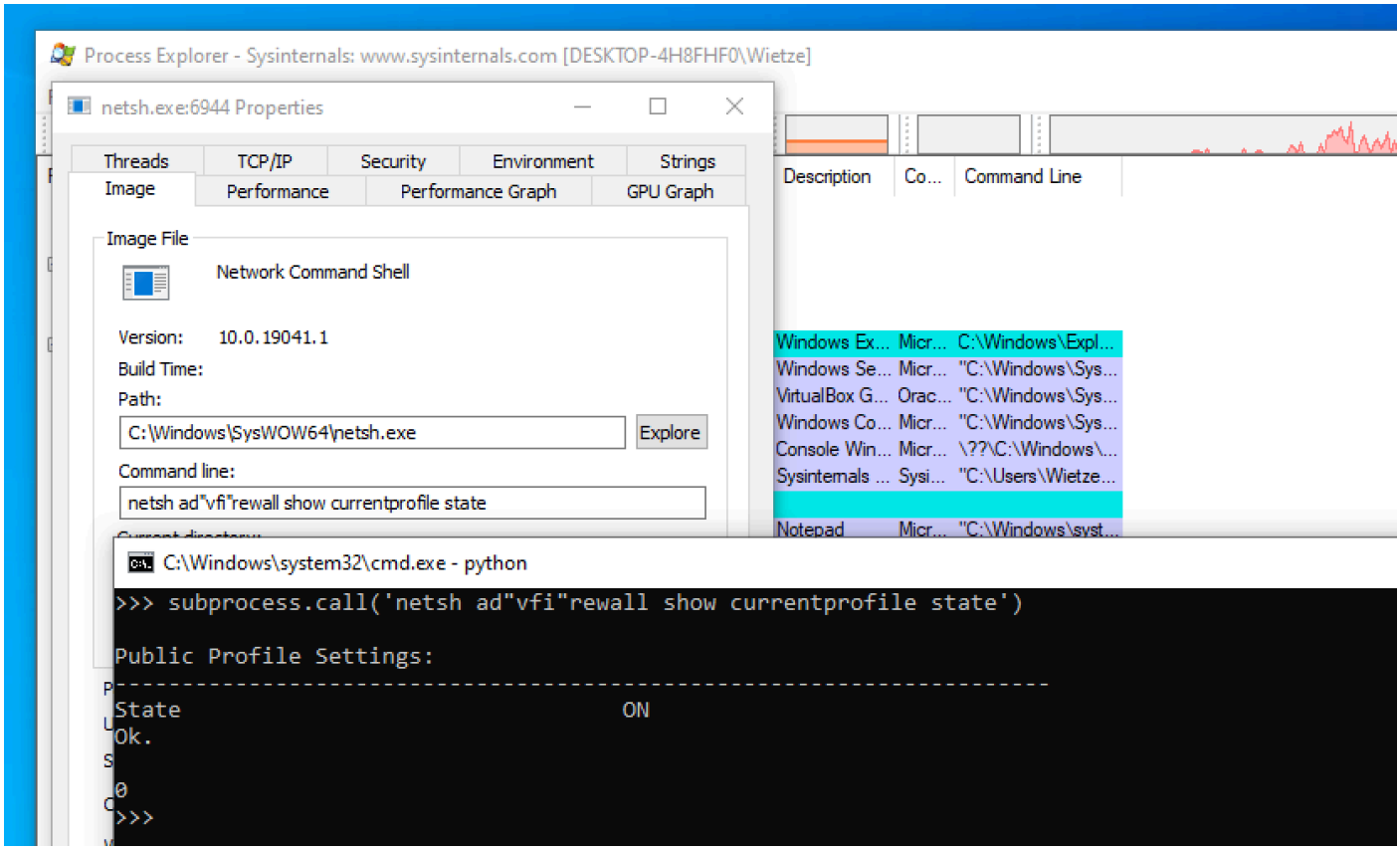


`wevtutil gچli hardwareevents`

`dir "c:\windows\"`

`dir c:\windows\`

```
dir c:\"win"d""ow"s"
```



netsh ad"vfi"rewall show currentprofile state

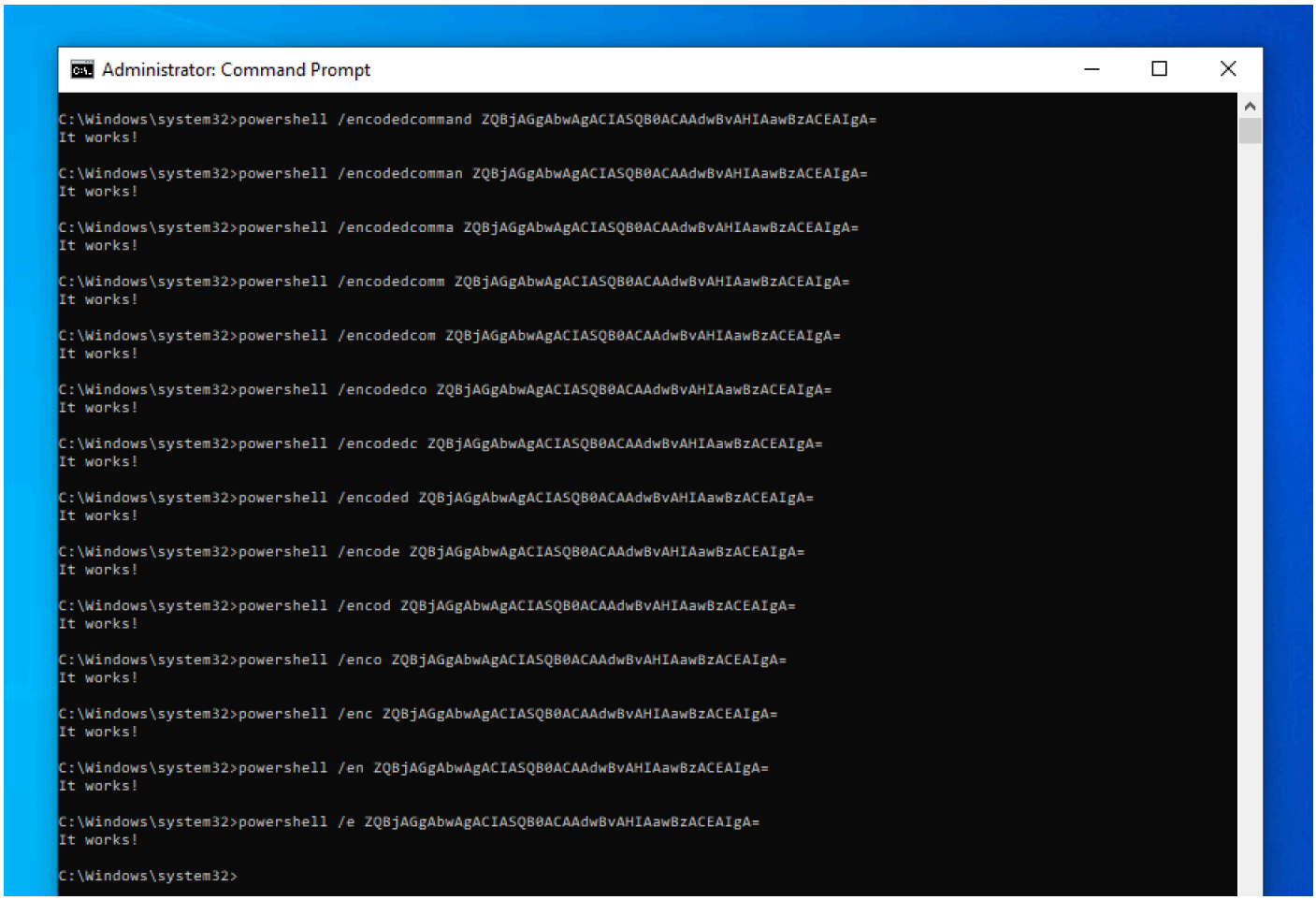
cmd

```
netsh ad""vfi""rewall show currentprofile state
```

grep -i keyword grep --ignore-case keyword

cmdkey /l cmdkey /list

wevtutil gli wevtutil get-loginfo



`powershell /encodedcommand ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=`

`/e`

`/noprofile` `/nop` `/no` `/noexit` `/ec`

`/encodedcommand`

`arp.exe`					
`at.exe`					
`bitsadmin.exe`					
`cacls.exe`					
`certutil.exe`					
`cmdkey.exe`					
`cmstp.exe`					
`csc.exe`					
`curl.exe`					
`findstr.exe`					
`fltmc.exe`					
`forfiles.exe`					
`icacls.exe`					
`ipconfig.exe`					
`jsc.exe`					

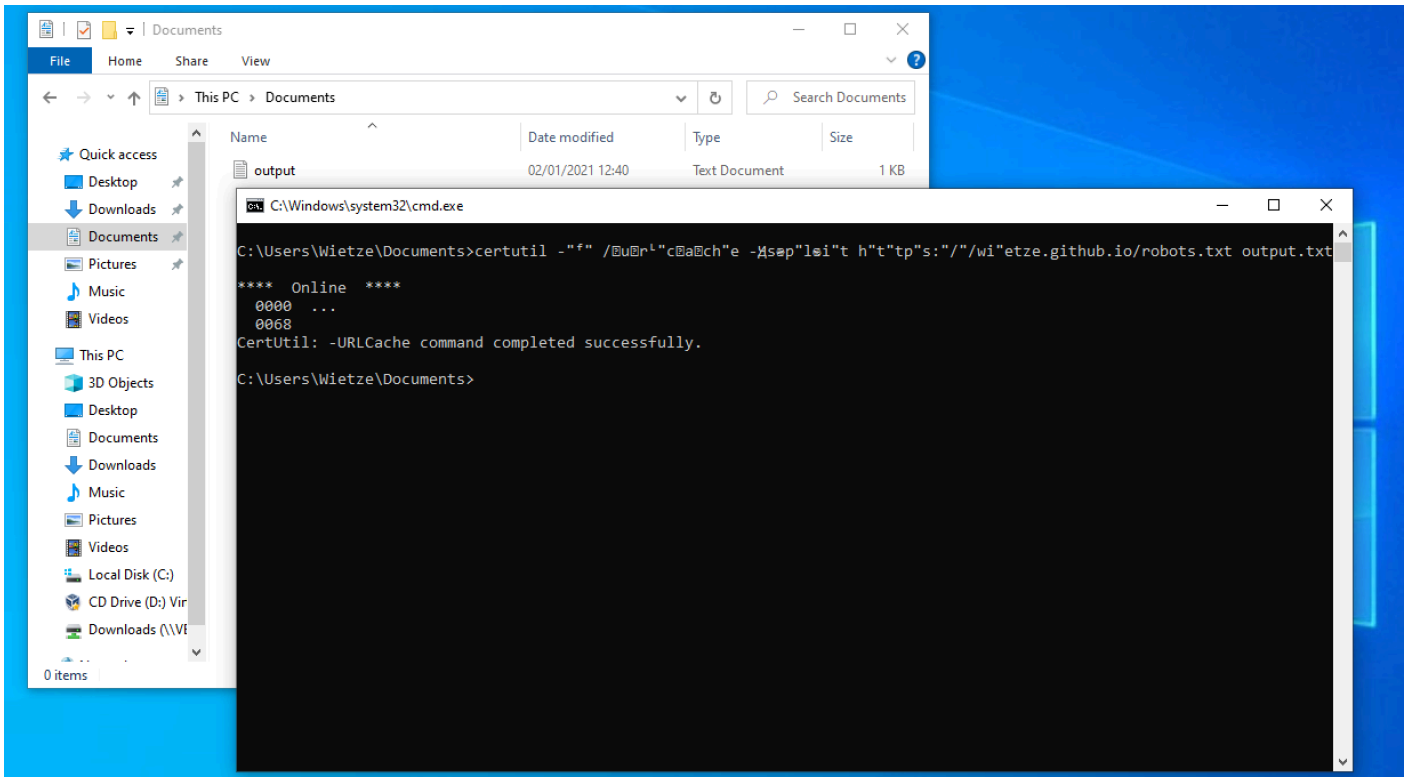
`nslookup -querytype=ALL (...)`

`nslookup` `-q`

`certutil` `urlcache` `f`

```
detection:
    selection:
        Image: "*\\certutil.exe"
        CommandLine|contains|all:
            - "/urlcache"
            - "/f"
    condition: selection
```

`-urlcache` `/urlcache` `/urlcache` `/url"cach"e` `-u r"c a ch"e`



certutil -f -urlcache -split https://wietze.github.io/robots.txt output.txt

```yaml
detection:
    selection:
        Image: "*\\certutil.exe"
        CommandLine|contains|all:
            - "urlcache"
            - "f"
    condition: selection
```

`urlcache` `/urlcache` `f` `/f`

`[-/\\]`

```yaml
detection:
    selection:
        Image: "*\\certutil.exe"
        CommandLine|re: "^(?=.*[-/\\]urlcache)(?=.*[-/\\]f).+.*"
    condition: selection
```

`wevtutil` `wevtutil`
