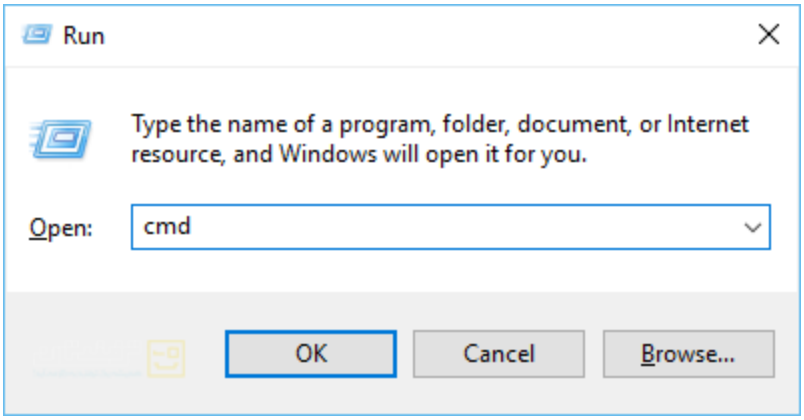
مفیدترین دستورات CMD برای هکرها

خط فرمان یا Command Prompt یکی از ابزارهای کاربردی هکرها محسوب می‌شود. در این ترفند به معرفی دستوراتی خواهیم پرداخت که توسط هکرها بیشترین استفاده را دارند.

برای دسترسی به CMD کافی است کلیدهای ترکیبی Win+R را فشار دهید تا Run باز شود. سپس عبارت cmdرا وارد کرده و Enter بزنید.



۱. ping

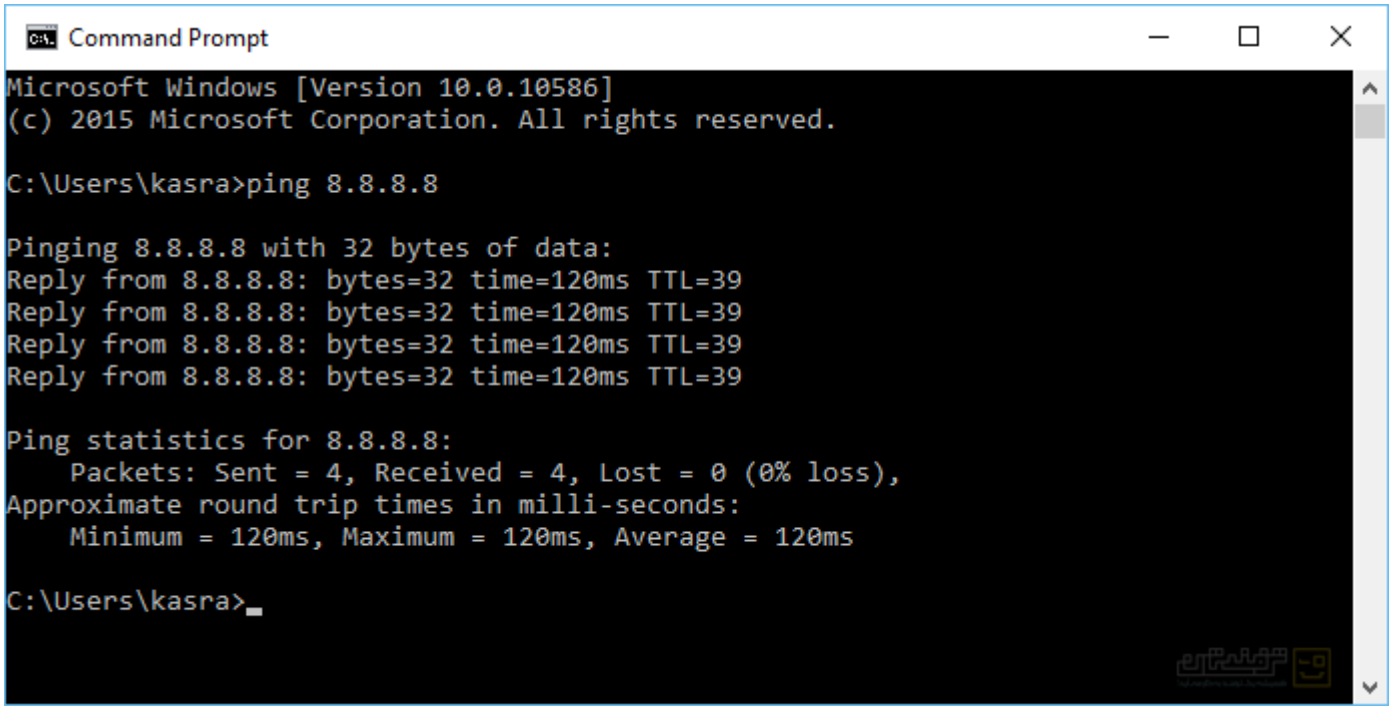
این دستور به شما اجازه می‌دهد که پی ببرید میزبان مورد نظر شما در حال حاضر دردسترس است یا خیر. بدین معنا که به هنگام اجرای دستورping ، میزبان در صورت متصل بودن چه پاسخی را برای شما ارسال می‌کند.

برای استفاده از این دستور کافی است عبارت ping را به همراه IP یا دامنه‌ی سایت یا کلاینت مورد نظر وارد نمایید. به عنوان مثال:

ping ۸.۸.۸.۸

ping www.google.com

پاسخ دریافتی از میزبان بیان‌گر وضعیت آن است. هر چه زمان درج شده در مقابل time، کم‌تر باشد و پاسخ دریافتی عاری از خطا باشد، به این معناست که سرعت اتصال به آن بیشتر و وضعیت آن نیز پایدارتر است.



۲. nslookup

این دستور کاربردهای گوناگونی دارد. یکی از آن‌ها یافتن IP از روی DNS است. فرض کنید آدرس یک سایت را می‌دانید اما از IP آن بی‌خبر هستید. با استفاده از این دستور می‌توانید به IP هر سایتی پی ببرید. به عنوان مثال:

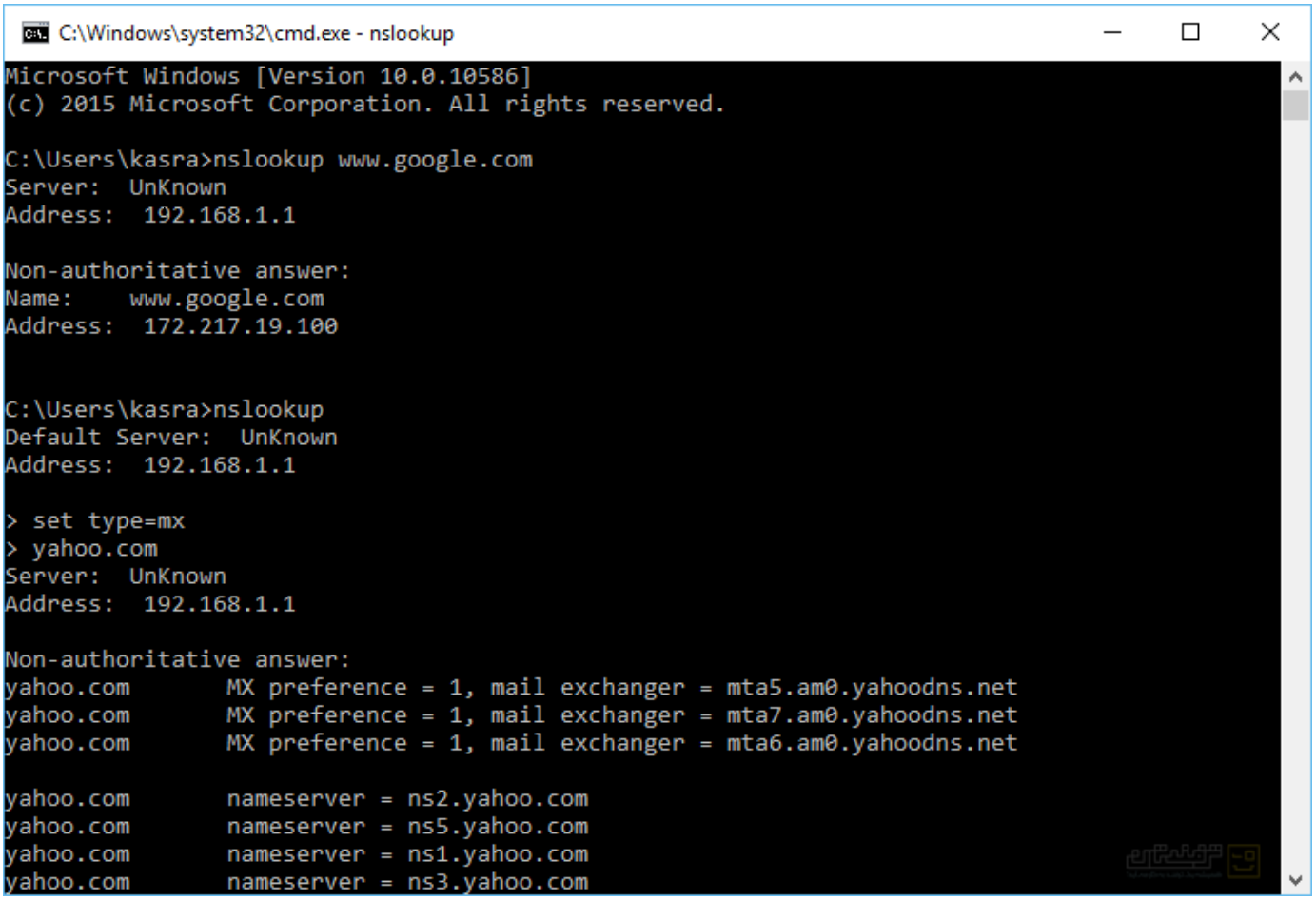
nslookup www.google.com

یکی دیگر از کاربردهای nslookup در یافتن IP یک میل سرور خاص است. به عنوان مثال برای یافتن IP میل سرورهای یاهو این دستورات بایستی به ترتیب وارد شوند:

nslookup

set type=mx

yahoo.com



۳. tracert

با استفاده از این دستور می‌توانید از مسیری که یک بسته در شبکه طی می‌کند تا به مقصد برسد اطلاعات خوبی کسب کنید. این دستور (ترفندستان) برای مسیریابی بسته‌ی ارسالی تا مقصد بسیار مفید است.

مثال:

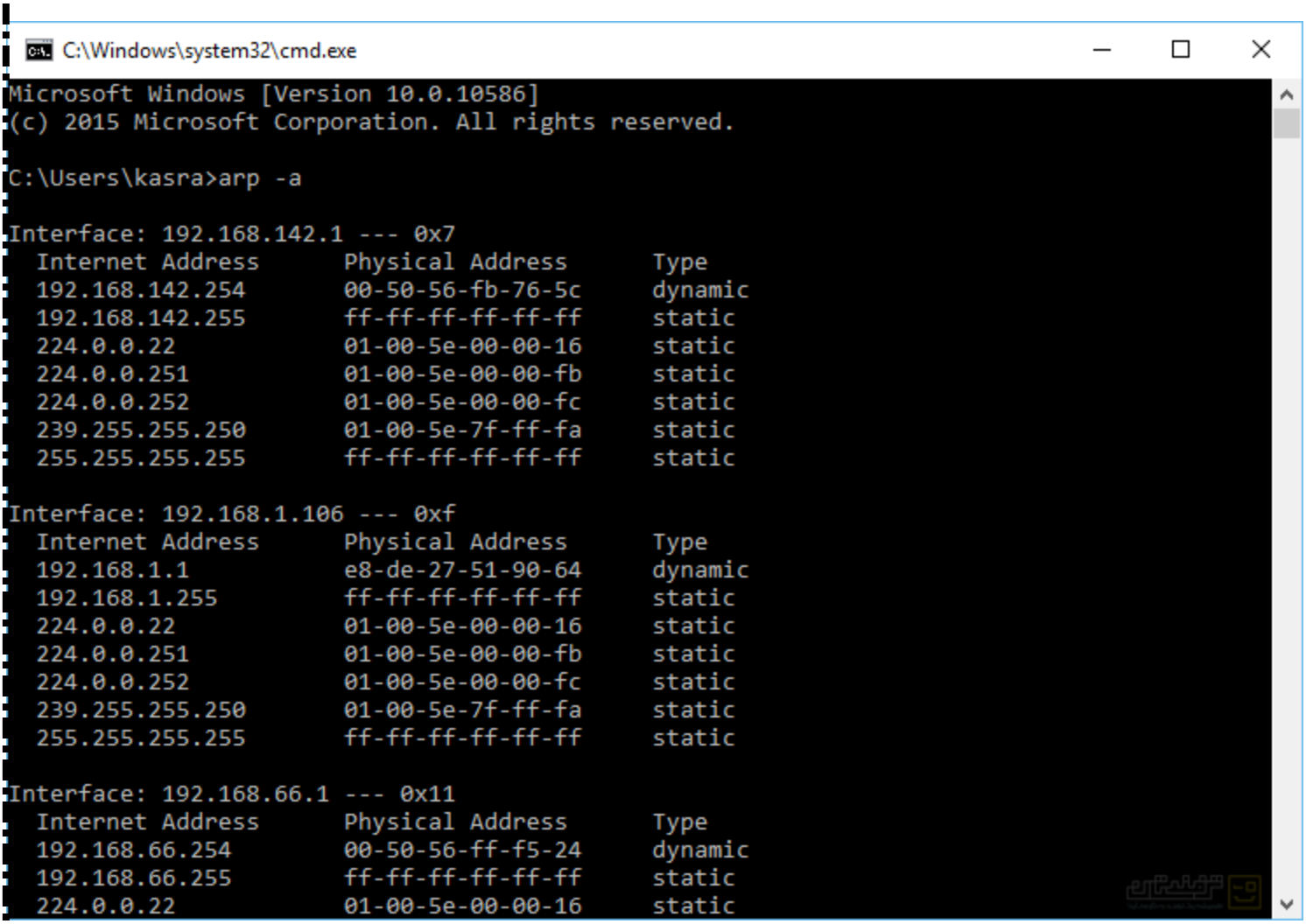
tracert ۸.۸.۸.۸

tracert www.google.com

۴. arp

این دستور جدول arp را برای شما نمایش می‌دهد. در این جدول، IPها و آدرس معادل MAC آن‌ها نگهداری می‌شوند. اگر فعالیت غیرقانونی در شبکه‌ی شما رخ داده است و به عنوان مثال کارت شبکه‌ای بدون اجازه‌ی شما تعویض شده است، از طریق این جدول می‌توانید به سادگی به این موضوع پی ببرید:

arp -a



۵. route

این دستور اطلاعات کامل مربوط به لیست کارت‌های شبکه، جدول مسیریابی و درگاه‌های هر یک را برای شما بازگو می‌کند:

route print

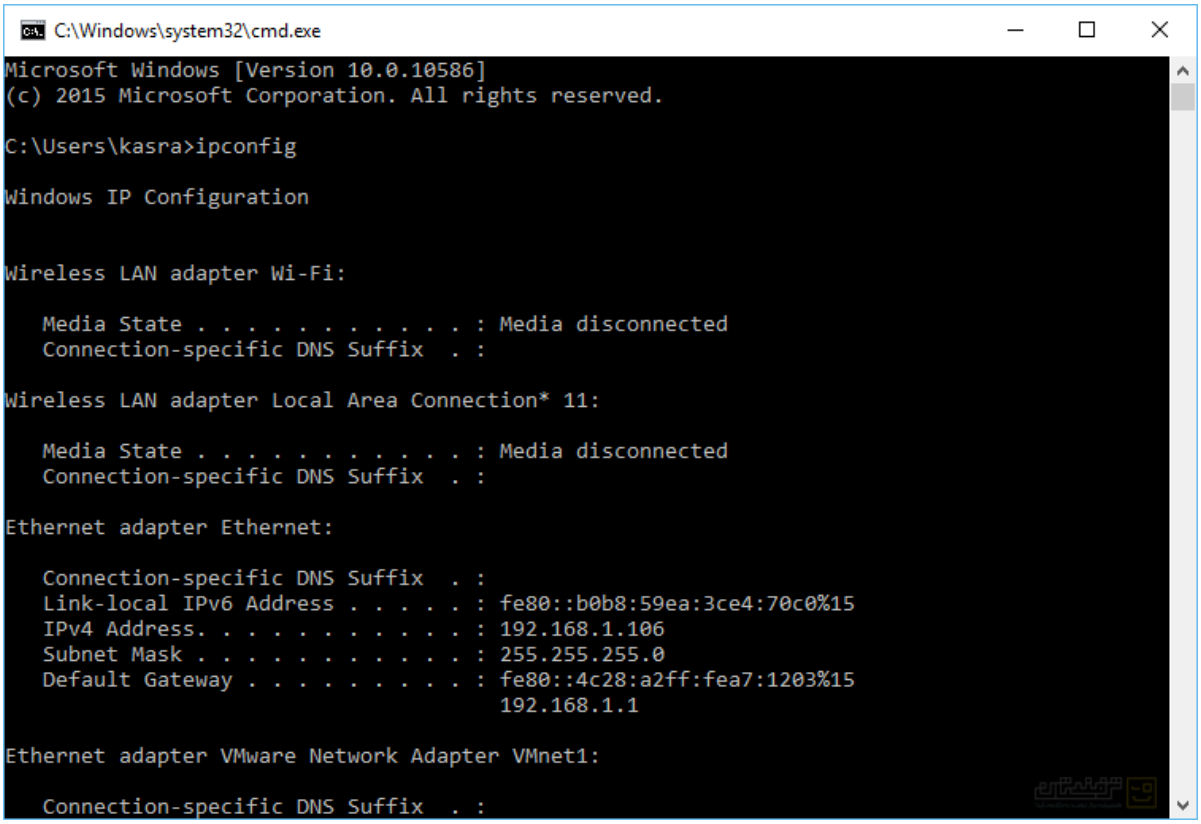
۶. ipconfig

این دستور اطلاعات مفیدی در خصوص IP و Gateway شما، DNSدر حال استفاده و نظایر آن را برای شما نمایش می‌دهد:

ipconfig

یا

ipconfig /all



همچنین اگر از IP دینامیک استفاده می‌کنید و مایلید IP خود را تغییر دهید با این دستورات می‌توانید این کار را انجام دهید:

ipconfig /release

ipconfig /renew

۷. netstat

این دستور وضعیت اتصالات شما را نمایش می‌دهد:

netstat

نمایش تمامی پورت‌هایی که در وضعیت شنود قرار دارند و اتصال با نام:DNS

netstat -a

نمایش تمامی اتصالات باز و IP آن‌ها:

netstat -n

ترکیب دو حالت بالا:

netstat -an

دستور زیر نیز تمامی پوشه‌های به اشتراک‌گذاشته‌شده در رایانه‌ی مقصد را نمایش می‌دهد:

net view x.x.x.x

یا

net view computername

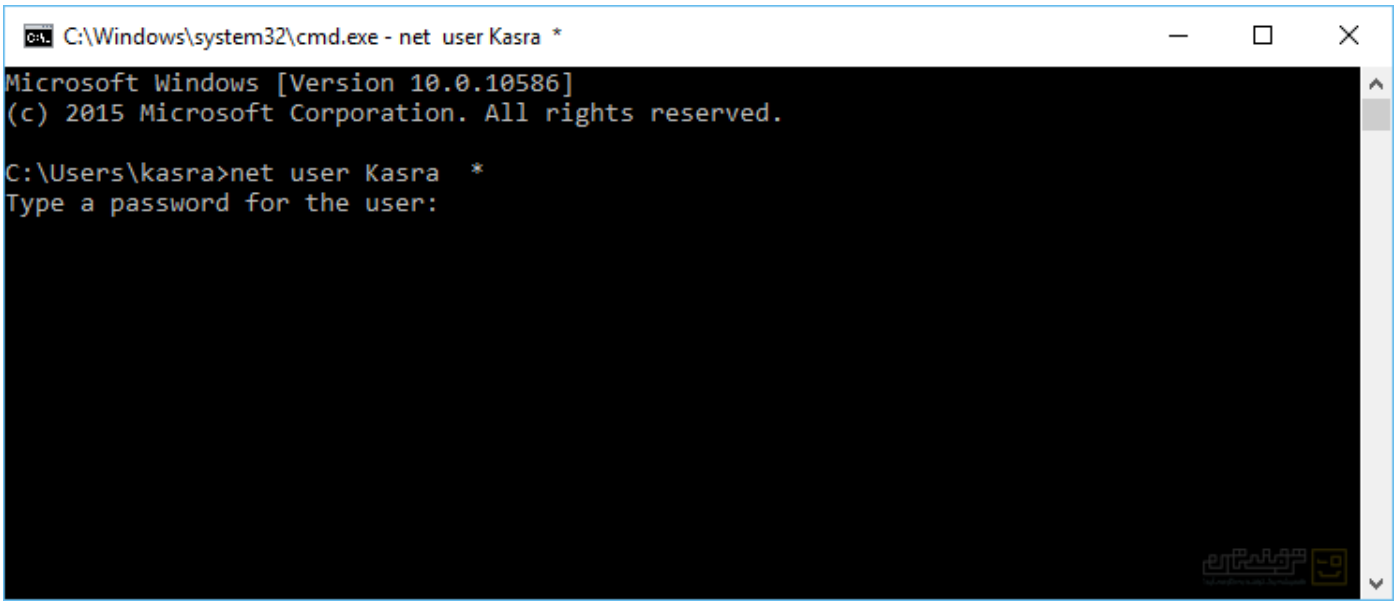
به جای x.x.x.x و computername بایستی آدرس IP یا نام رایانه را وارد نمایید.

۸. netuser

این دستور رمز عبور حساب کاربری ویندوز را بدون دانستن رمز قبلی تغییر می‌دهد:

net user Tarfandestan *

به جای Tarfandestan نام کاربری ویندوز را بنویسید و پس از فشردنEnter ، رمز جدید را وارد کنید.



۹. سایر دستورات

دستورات دیگری نیز هستند که می‌توانند به شما کمک کنند.

اتصال به دستگاه مقصد با دسترسی:Administrator

net use \ipaddressipc$ “” /user:administrator

به جایipaddress ، آدرس IP را وارد نمایید.

پس از اتصال به مقصد اگر مایل به مرور کل درایو C بودید از این دستور استفاده کنید:

net use K: \computernameC$

به جای computername نام رایانه را وارد کنید. این دستور موجب ایجاد یک درایو مجازی می‌شود. دقت کنید این دستور زمانی کار می‌کند که رایانه‌ی مقصد رمز عبور Adminastrator تعیین نکرده باشد.

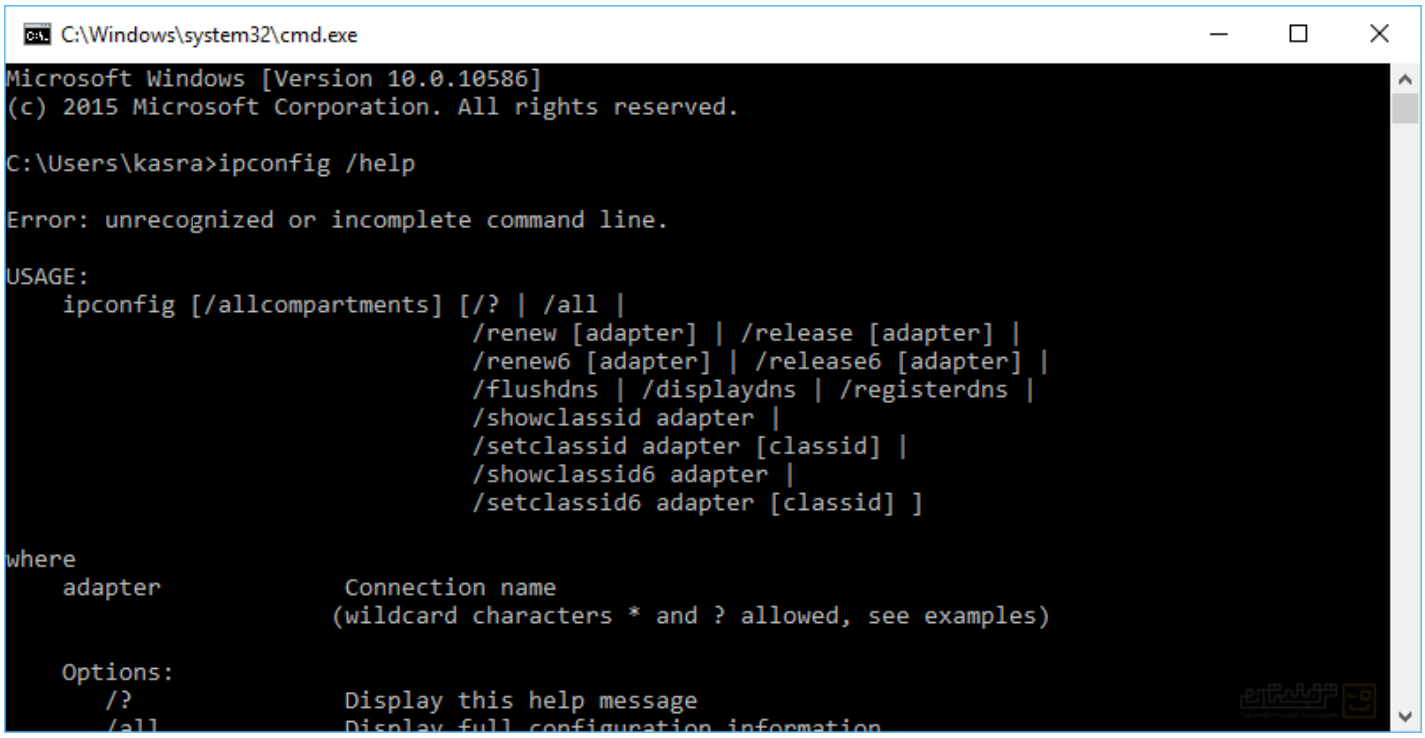
و در نهایت دستور Help برای دریافت راهنمایی:

command /help

یا

command /?

به جای command دستور مورد نظر را بایستی وارد نمایید. با این دستور می‌توانید پی ببرید هر دستور، چه کارایی و چه جزئیاتی دارد.


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\kasra>ipconfig /help
Error: unrecognized or incomplete command line.
USAGE:
ipconfig [/allcompartments] [/? | /all |
/renew [adapter] | /release [adapter] |
/renew6 [adapter] | /release6 [adapter] |
/flushdns | /displaydns | /registerdns |
/showclassid adapter |
/setclassid adapter [classid] |
/showclassid6 adapter |
/setclassid6 adapter [classid]]
where
adapter Connection name
(wildcard characters * and ? allowed, see examples)
Options:
/? Display this help message