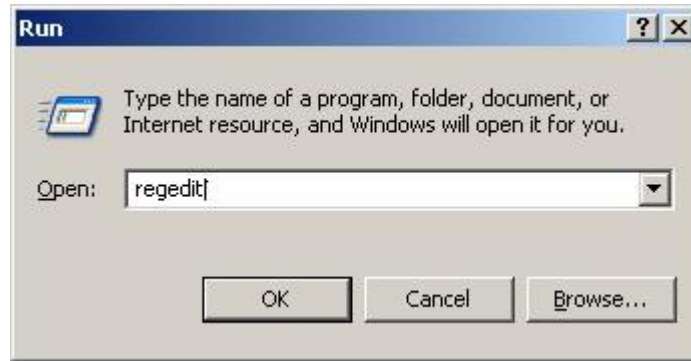


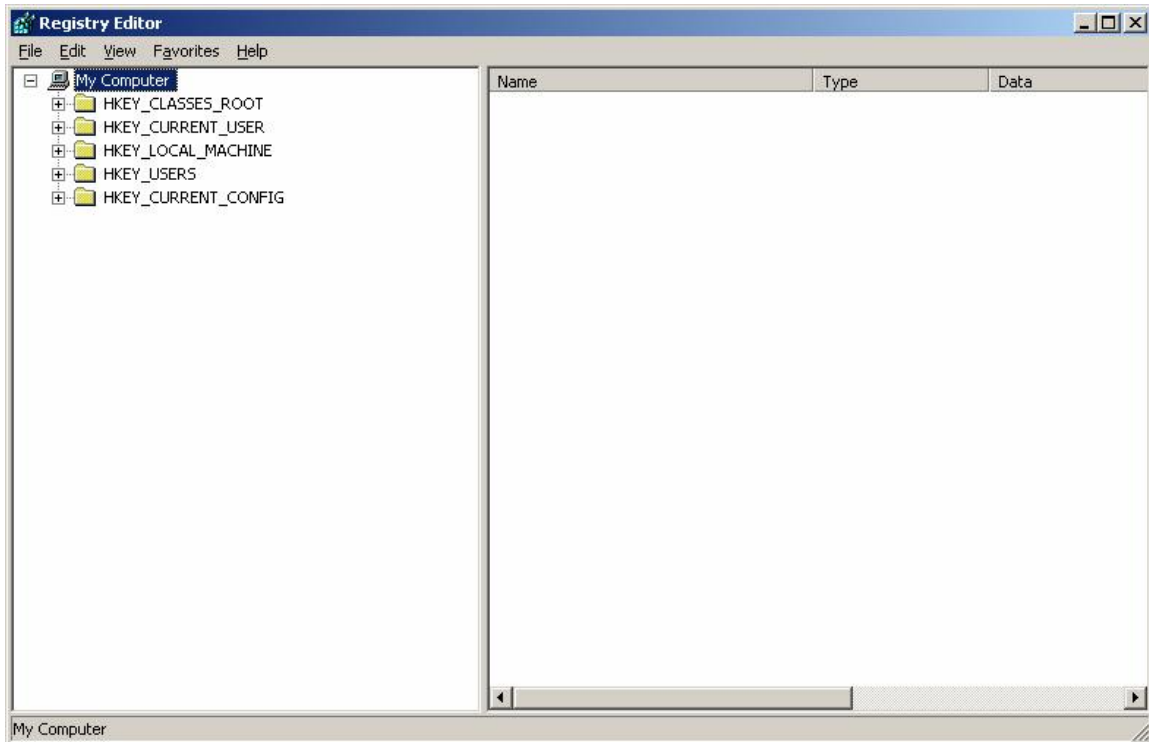
## بسمه تعالي

براي هك كردن ويندوز توسط يك فايل رجیستري این مراحل را دنبال می کنیم :

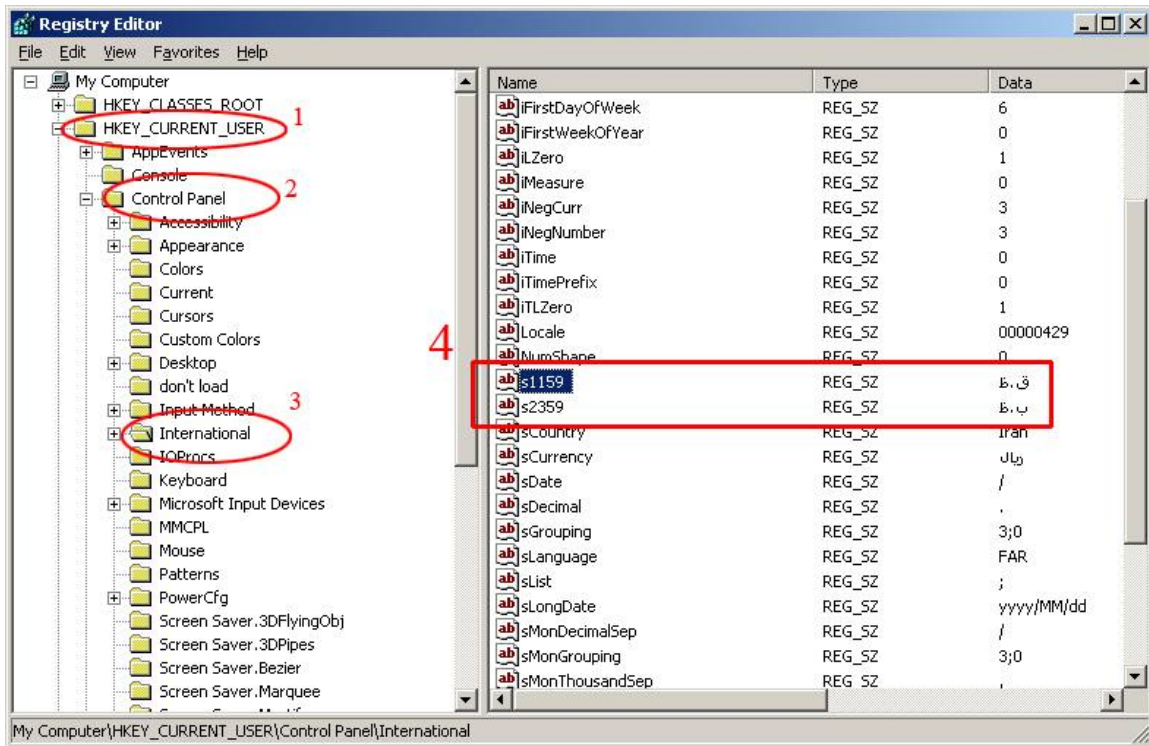
1- ابتدا وارد رجیستري شده (regedit) را در run نوشته و enter بزنید) سپس به آدرس مورد نظر بروید :



2- بعد از ظاهر شدن صفحه regedit به کلید یا محل و آدرس مورد نظر بروید :

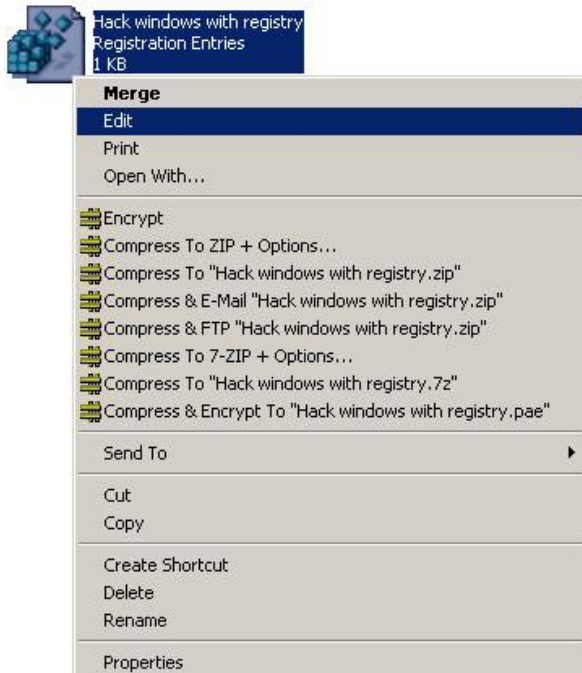


3- در این مثال می خواهیم با اجرای فايل ساخته شده نوشته کنار ساعت را به نوشته دیگری تغییر دهیم، برای این کار ابتدا به آدرسي که در عکس نمایش داده شده رفته و طبق مرألي که در زیر توضیح داده شده عمل کنید :



آدرسي که عکس نشان مي دهد در واقع بصورت زیر در فایلي که مي خواهيم بسازيم ديده مي شود :  
[HKEY\_CURRENT\_USER\Control Panel\International]

خوب از این جا ديگه اصل کار شروع مي شه لطفاً بيشتتر دقت کنيد : (^ + ^)  
1- روي گزینه s1159 و s2359 دابل کلیک کنيد يا راست کلیک کرده و modify را انتخاب کنيد حالا هر نوشته اي بجاي نوشته قبلي وارد کرده و ok را بزنييد، مي بينيد که نوشته ها عوض شده اند .  
2- حالا يکي از آن دو گزینه را انتخاب کرده و از منوي File گزینه Export... را کلیک کرده سپس محلي را که مي خواهيد اين فايل ذخيره شود را انتخاب و بعد در قسمت File name نامي براي فايلتان تايپ و کلید Save را کلیک کنيد.  
راستي دقت کردین که این فايل با پسوند reg ذخيره شد، حالا به محلي که فايلتان را ذخيره کرديد برويد و طبق مراحل زیر عمل کنيد :



1- روي فايل مورد نظر راست کلیک کرده و Edit را انتخاب مي کنيم تا آن را ويرايش کنيم.

2- فایل شما در Notepad باز شده و پر از نوشته و مقادیر عددی و کاراکتری است، خوب کار شما این وسط چیست الان می گم ، شما طبق عکس نوشته را ویرایش می کنید، توجه کنید :



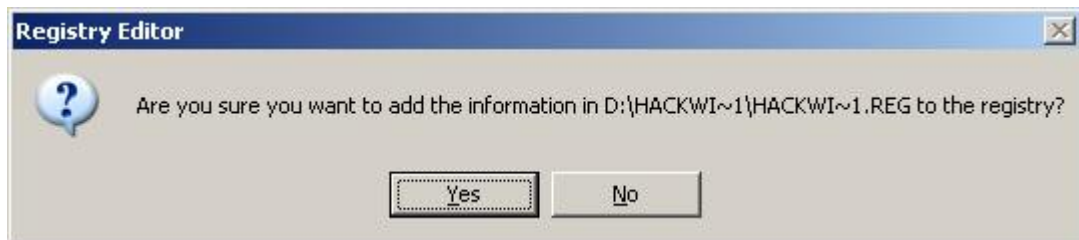
The screenshot shows a Notepad window titled "Hack windows with registry - Notepad". The text inside is a registry script for the Windows Registry Editor. The path "[HKEY\_CURRENT\_USER\Control Panel\International]" is highlighted with a red box. The script contains various registry values for international settings. Two values, "s1159" and "s2359", are also highlighted with red boxes. Overlaid on the script is Persian text in red: "لطفا توجه کنید ما فقط آن قسمتهایی که با مستطیل قرمز مشخص شده اند را احتیاج داریم پس بقیه خطها را می توانید پاک کنید چون با آنها کاری نداریم".

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Control Panel\International]
"iCountry"="981"
"iCurrDigits"="2"
"iCurrency"="2"
"iDate"="2"
"iDigits"="2"
"iLZero"="1"
"iMeasure"="0"
"iNegCurr"="3"
"iTime"="0"
"iTLZero"="1"
"Locale"="00000429"
"s1159"="ز.ب."
"s2359"="ب.ب."
"Country"="Iran"
"Currency"="ت.د."
"Date"="/"
"Decimal"="."
"Language"="FAR"
"List"=";"
"LongDate"="yyyy/MM/dd"
"ShortDate"="yyyy/MM/dd"
"Thousand"=","
"Time"=":"
"TimeFormat"="hh:mm:ss tt"
"TimePrefix"="0"
"MonDecimalSep"="/"
"MonThousandSep"=","
"NegNumber"="3"
"NativeDigits"="۰۱۲۳۴۵۶۷۸۹"
"NumShape"="0"
"CalendarType"="2"
"FirstDayofWeek"="6"
"FirstweekofYear"="0"
"Grouping"="3;0"
"MonGrouping"="3;0"
"PositiveSign"=""
"NegativeSign"="-"

[HKEY_CURRENT_USER\Control Panel\International\Geo]
"Nation"="116"
```

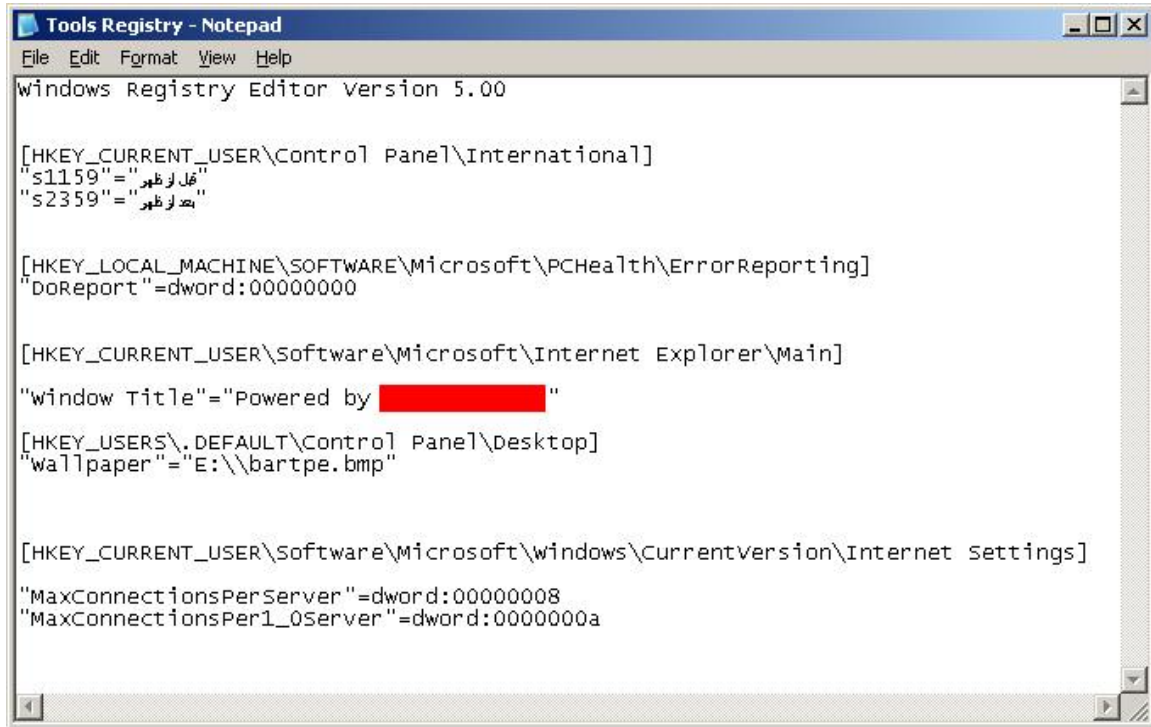
2- حالا فایلتان را ذخیره کرده و اجرا کنید پیغام زیر نمایش داده می شود :



این پیغام میگوید که مطمئن هستید که می خواهید این اطلاعات در رجیستری اعمال شود، پس شما Yes را کلیک کنید تا اولین ویندوز هکینگ شما در ویندوز اعمال شود .

خوب حالا نکاتی که بعد از این تمرینها خیلی مهم هستند اینها هستند :

- 1- از این به بعد آگه فیل ساخته شده را روی هر سیستمی که ویندوز xp داشته باشد اعمال کنید نوشته کنار ساعت عوض خواهد شد .
- 2- ویروس نویسان و تروجان نویسان از این طریق برای اینکه ویروس یا تروجان روی سیستم هدف در هربار راه اندازی اجرا شود استفاده می کنند .
- 3- ما برای اینکه شبهه ویروسهایمان را روی سیستم هدف در هر بار راه اندازی اجرا کنیم از این روش استفاده می کنیم.
- 4- برای گسترش فایل ویندوز هکینگ طبق عکس زیر کلیدها را اضافه کنید :



```
Tools Registry - Notepad
File Edit Format View Help
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Control Panel\International]
"s1159"="غل زظور"
"s2359"="هد زظور"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting]
"DoReport"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"window Title"="Powered by ██████████"

[HKEY_USERS\.DEFAULT\Control Panel\Desktop]
"wallpaper"="E:\\bartpe.bmp"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
"MaxConnectionsPerServer"=dword:00000008
"MaxConnectionsPer1_0Server"=dword:0000000a
```

موفق و پیروز باشید گروه امنیتی و پژوهشی Cyber Quest

تمام حقوق این مقاله متعلق به گروه امنیتی و پژوهشی Cyber Quest دارد . استفاده از این مقاله با ذکر نام گروه مجاز می باشد .