بنية الحاسب

حماية الجهاز من الفايروسات و الاختراقات

الوحدة الثانية : حماية الجهاز من الفايروسات و الاختراقات

الهدف العام للوحدة :

أن يكون المتدرب قادراً على العمل على برامج الحماية من الفايروسات .

الأهداف الإجرائية :

- أن يكون المتدرب قادراً على العمل على تركيب برامج الحماية من الفايروسات .
- أن يكون المتدرب قادراً على معرفة طريقة عملها .
- أن يكون المتدرب قادراً على معرفة طرق الوقاية من الفايروسات.

الوقت المتوقع لإتمام الوحدة : 16 حصة .

حماية الجهاز من الفايروسات و الاختراقات

نبذة:

يتطلب جهاز الحاسب الآلي أحد البرامج الهامة لحماية بياناتك و ملفاتك من الإتلاف أو التلاعب بها أو ضرراً على جهازك، لذلك انتشرت البرامج المتخصصة في هذا المجال.

فايروسات الحاسب(computer viruses):

شكليا .. قطعة من شفرة البرنامج التي تعمل على نسخ نفسها في الجهاز .. برنامج أو جزء من برنامج ينظم إلى الانتشار من نظام إلى نظام آخر دون علم أو أذن من أصحاب النظام الذي ينتشر به ..

دودة الحاسب(computer worm):

هي برنامج حاسب منطوي بذاته مشابه لفيروس الحاسب .. الفرق الرئيس بينهما أن فيروس الحاسب يلصق بنفسه إلى ملفات .. ويكون جزء لا يتجزأ من برنامج تنفيذي .. بينما الدودة مستقلة بذاتها ولا تكون جزءًا من أي برنامج .. الدودة قد تكون مصممة لعمل عده أشياء مثل حذف(delete) ملفات على النظام أو إرسال وثائق عبر البريد الإلكتروني.

الوقاية من الفايروسات و التجسسات و إزالتها

لابد من الوقاية من الفايروسات المنتشرة وأخذ وسائل الأمان لتجنبها ،وعدم التهاون بها.و هناك عدة طرق هامه لتجنب الفايروسات و التجسسات ومنها:

1. التحديث التلقائي أو المتابعة لتحديث نظام التشغيل على جهاز الحاسب.
2. تجنب تحميل البرامج من مواقع الإنترنت غير المعتمده وغير الموثوق بها.
3. تنصيب أحد برامج الحماية ومتابعة تحديث البرنامج.
4. تجنب فتح الملفات، أو فتح رسائل البريد الإلكتروني من أشخاص غير موثوق بهم أو غير معروفين لديك.
5. استخدام نظام الملفات NTFS حيث يتميز بالأمان.
6. تجنب تسجيل الدخول باسم مستخدم موجود في مجموعة المدراء، عند تصفحك للإنترنت.

أعراض الإصابة بالفايروسات :

- النقص الشديد في الذاكرة . فعندما يبدأ الفيروس في العمل يحتل مواقع الذاكرة ويبدأ في تدميرها مما ينتج عنه صعوبة تشغيل البرامج المعتادة وتوقفها عن العمل.
- بطء تشغيل النظام بصورة مبالغ فيها.
- عرض رسائل الخطأ بدون أسباب حقيقية.
- تغيير عدد ومكان الملفات وكذلك حجمها دون أسباب منطقية.
- أحيانا ظهور أحرف غريبة عند النقر على لوحة المفاتيح.
- الحركة العشوائية للقرص الصلب

أماكن الإصابة :

ملف Command.com حيث إنه المسؤول عن استقبال أوامر التشغيل الداخلية . ملفات Autoexec.bat و Config.sys .والتي يبحث عنها النظام عند بدء التشغيل وينفذ ما بها من تعليمات .

أما أخطر الأماكن التي يتمركز بها الفيروس فهو مخزن CMOS وهو مكان التعليمات الأولى قبل التشغيل ومكان ضبط ساعة النظام ولذلك يستخدمه الفيروس لضبط ساعة وتوقيت الهجوم

أهم البرامج المضادة للفايروسات :

1. Symantec Norton Antivirus 2004
2. McAfee Virus Scan
3. F- Secure Anti- Virus
4. Sophos Anti- Virus
5. Panda Software Antivirus Platinum
6. Trend Micro Pc-Cillin

قائمة تمارين الوحدة :

- **التمرين الأول :** تثبيت برنامج Norton AntiVirus2004.
- **التمرين الثاني :** ضبط إعدادات برنامج Norton AntiVirus2004.
- **التمرين الثالث :** تحديث برنامج Norton AntiVirus2004 عبر الإنترنت .
- **التمرين الرابع :** استخدام Norton AntiVirus2004 لتفحص النظام .
- **أسئلة وتمارين نظرية** .

التمرين الأول

تنصيب و ضبط إعدادات البرنامج (Norton AntiVirus2004)

النشاط المطلوب: قم بتثبيت برنامج مكافحة الفايروسات **Norton AntiVirus2004**

الأدوات:

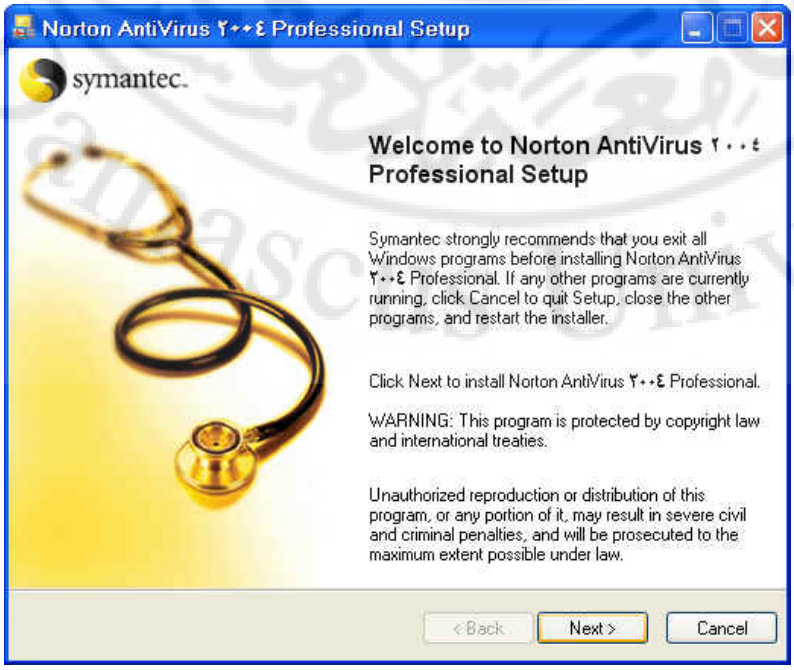
قرص برنامج مكافحة الفايروسات Norton AntiVirus2004

الخطوات:

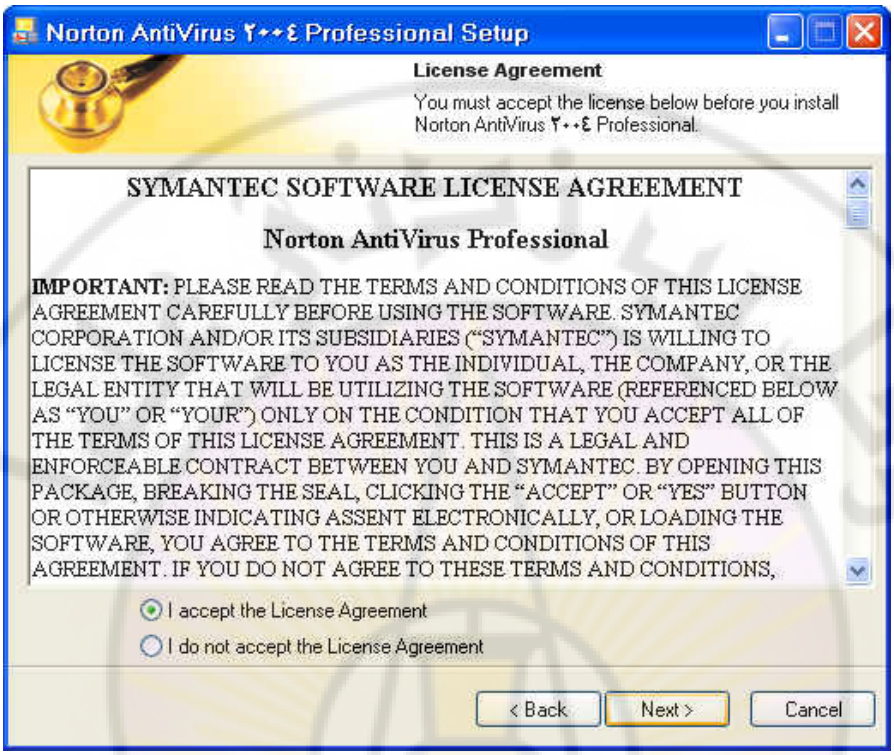
1. قم بفصل الإنترنت (مهم جدا)
2. ضع الأسطوانة الخاصة بالبرنامج داخل قارئ الأقراص ستكون القراءة تلقائية، (في حالة عدم القراءة تلقائية قم بالضغط على الملف **NAVSETUP.EXE**) ، ستظهر هذه النافذة:

وتعني (نعم) أنه سيقوم بفحص الجهاز، (لا) سيقوم بفتح النافذة الرئيسة للبدء في عملية التنصيب.

3. انقر على الزر (لا).
4. هذه أول خطوة لتحميل البرنامج . اضغط على التالي Next لمواصلة التحميل.

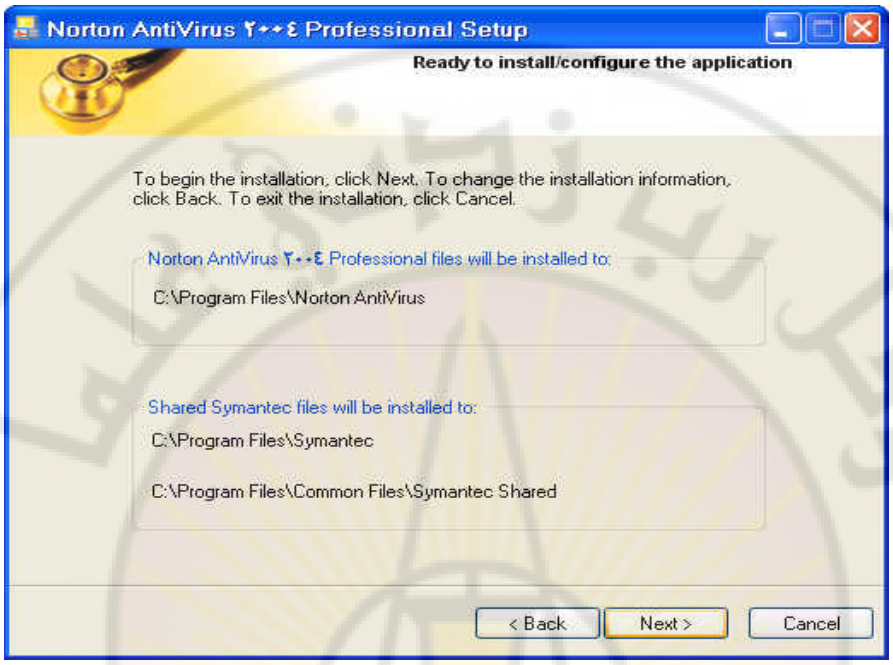


5. سؤال تأكيدي بأنه تمت قراءة جميع الشروط اختر.....I accept ثم اختر Next لمواصلة التحميل.

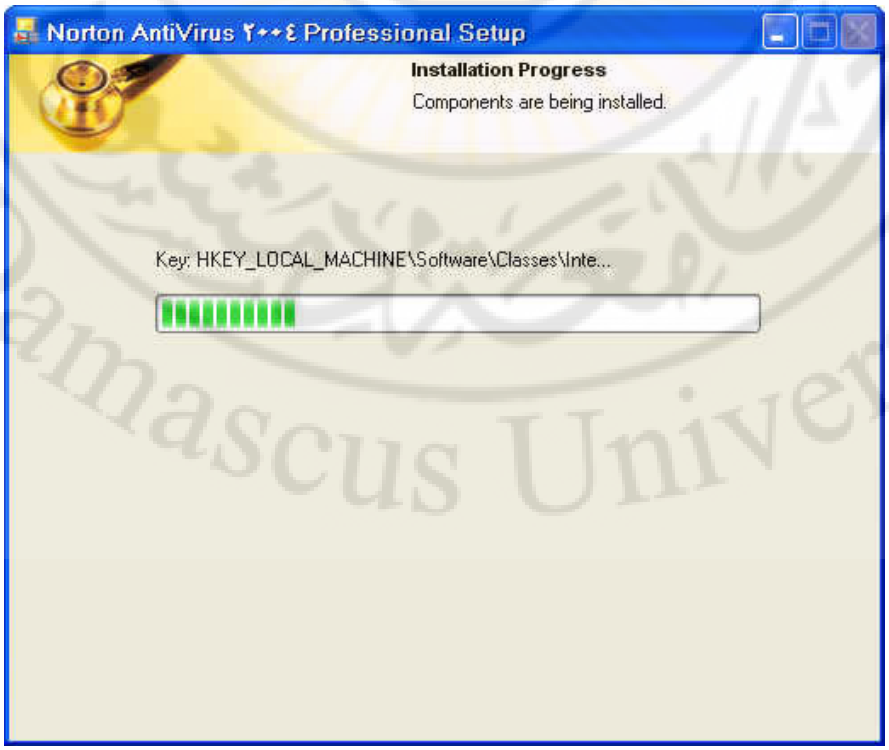


6. اختيار مكان حفظ البرنامج ، اختر Next ليتم حفظها في المسار المحدد في الصورة.

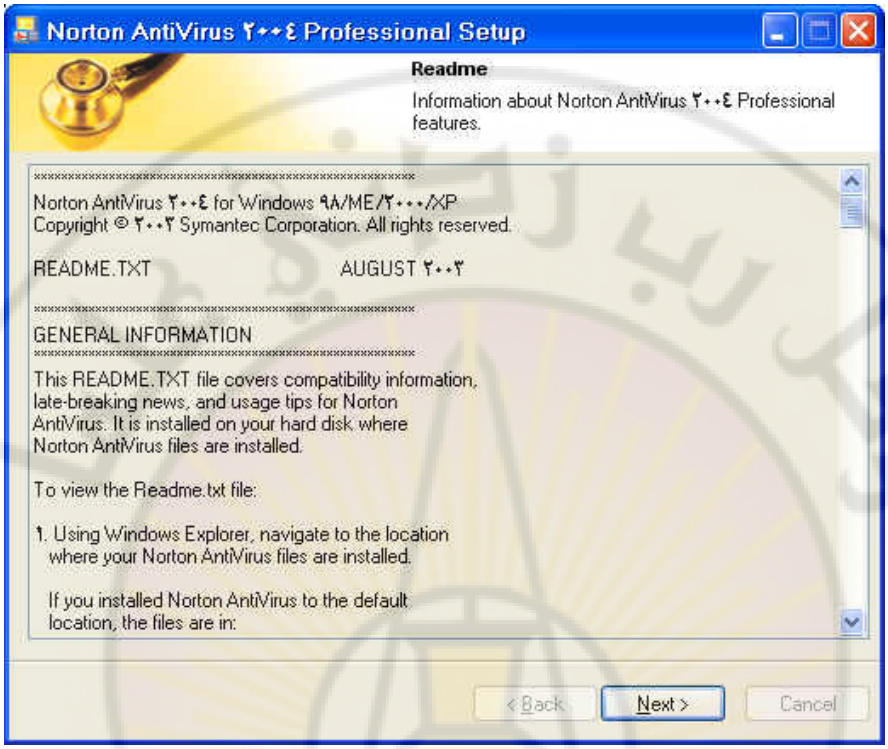
7. يطلب منك قراءة المعلومات عن مكان الحفظ لملفات البرنامج اضغط على Next لمواصلة التحميل



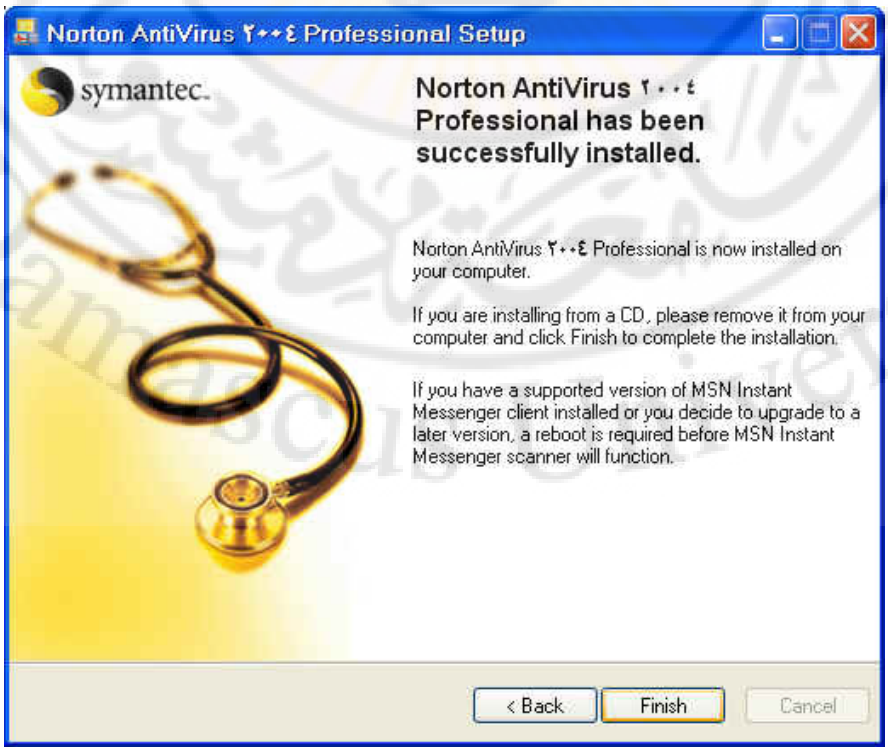
8. هذه الصورة تبين تحميل البرنامج التشغيلي بشكل سليم



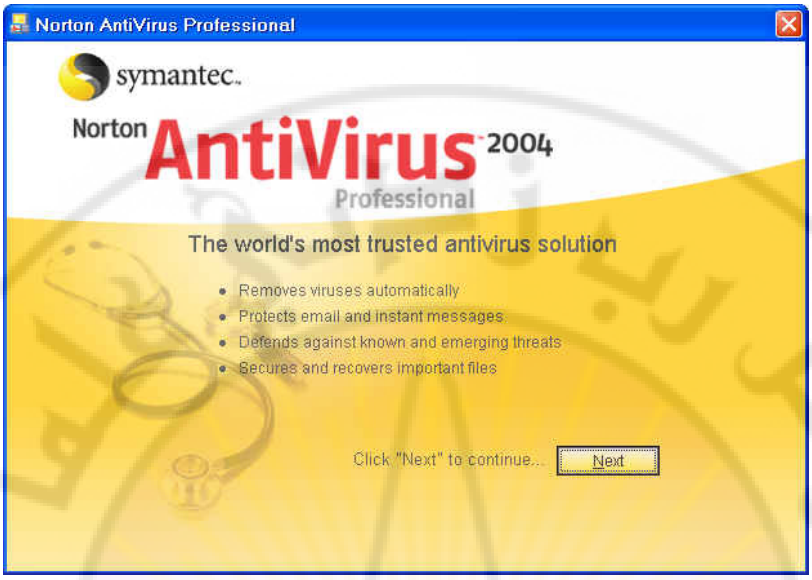
9. يطلب منك قراءة المعلومات عن هذا البرنامج اضغط على Next لمواصلة التحميل



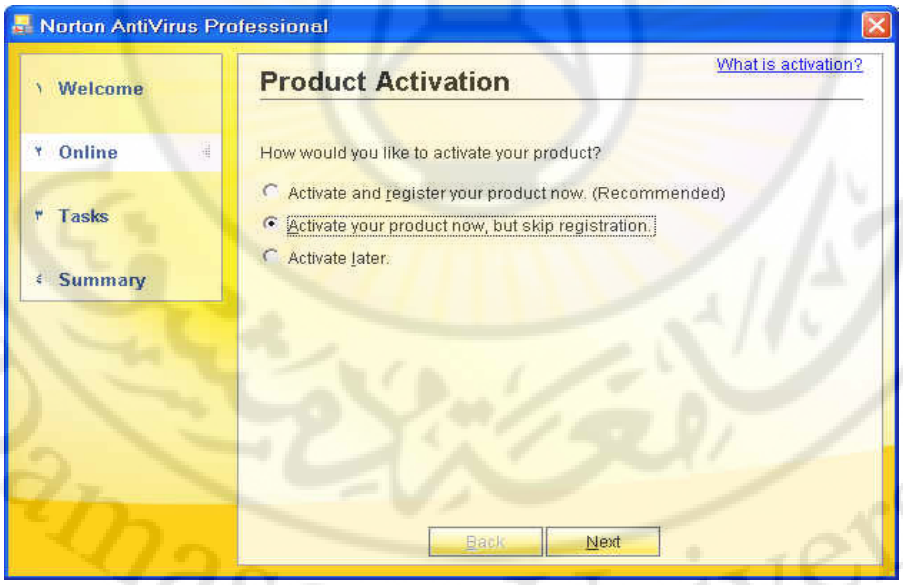
10. اضغط على Finish لإنهاء عملية التنصيب.



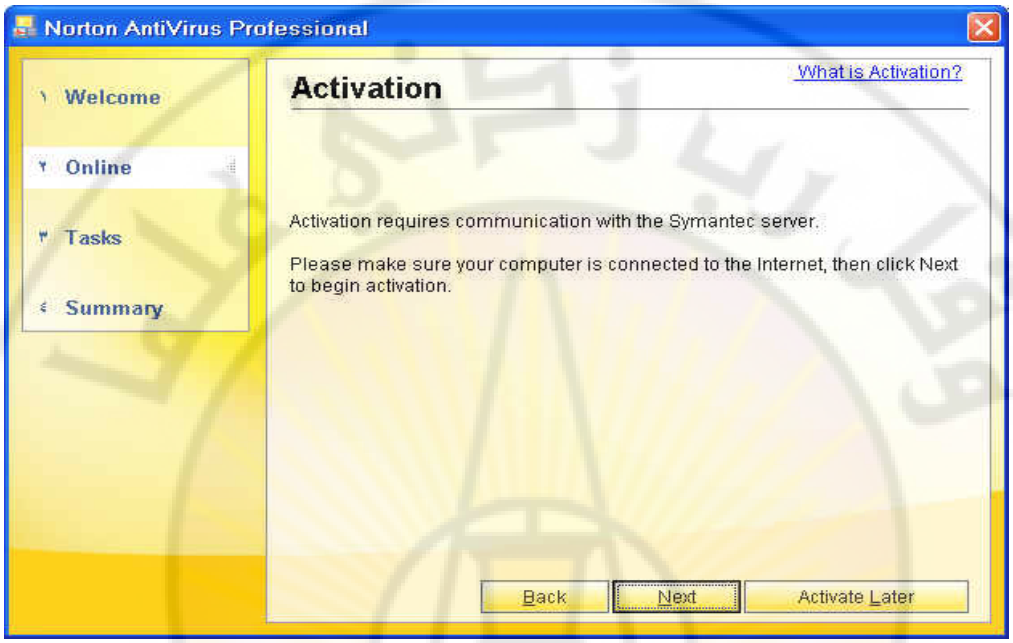
11. بعد تنصيب البرنامج تظهر شاشة لمرحلة أخرى وهي مرحلة تسجيل البرنامج.



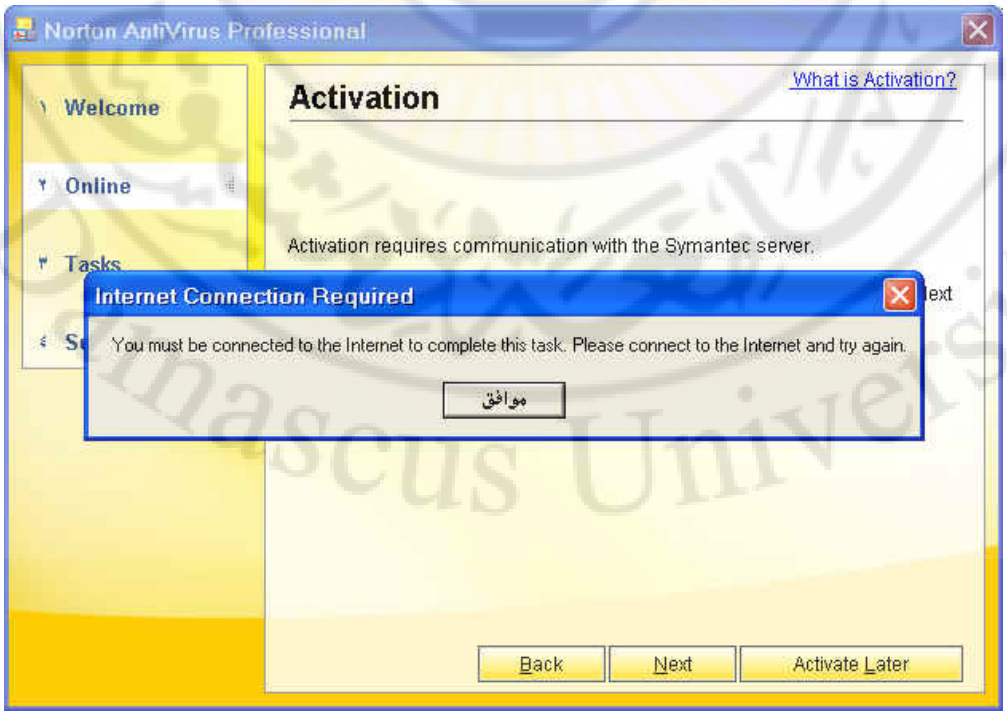
12. اضغط على التالي Next لمواصلة التحميل



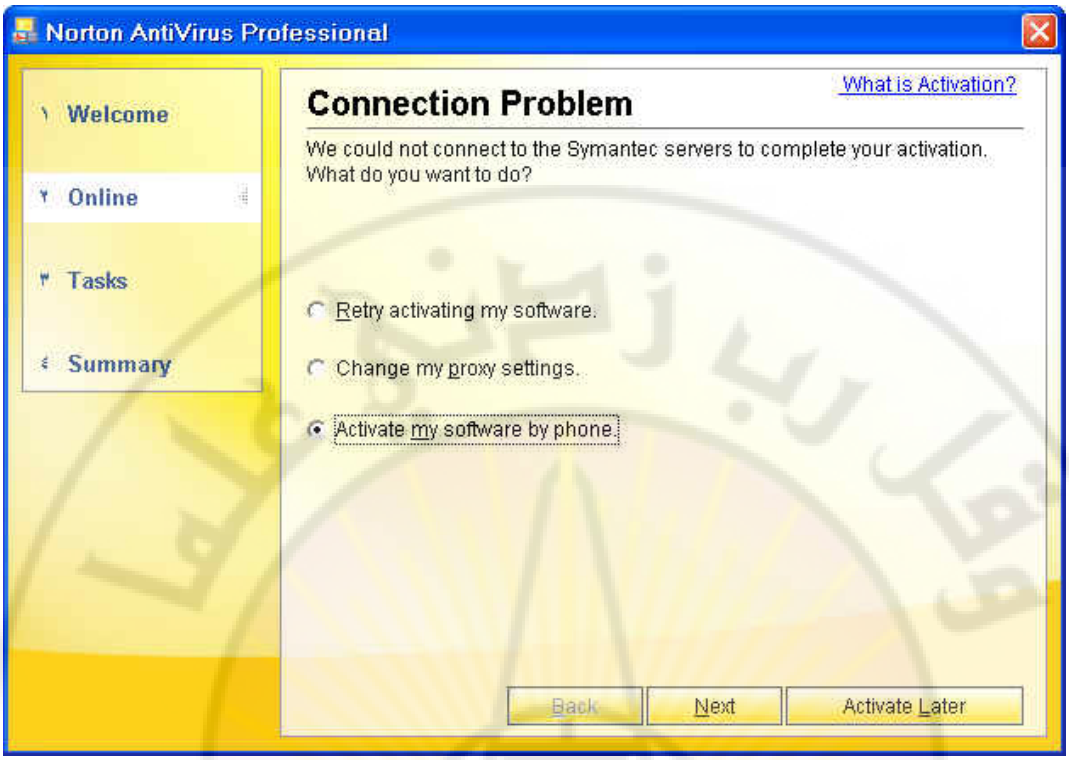
13. اختر(Activate your product now, but skip registration) وتعني تنشيط البرنامج الآن، ثم انقر NEXT



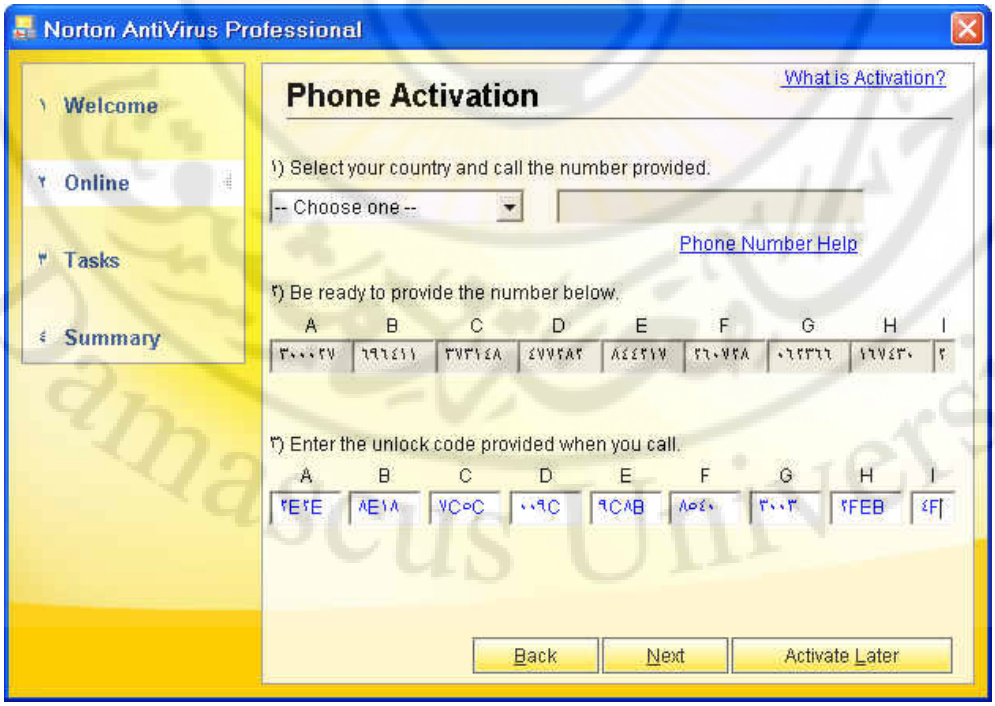
14. تبين هذه الرسالة بأنك لست متصلاً بالإنترنت تجاهلها واضغط NEXT



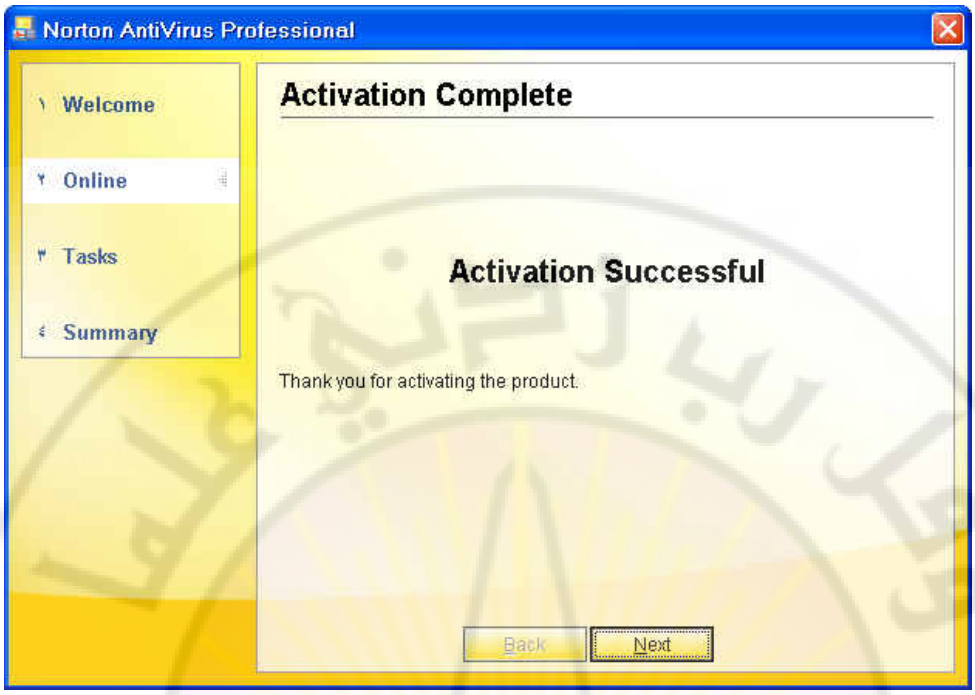
15. تبين هذه الرسالة بأنك لست متصلاً بالإنترنت تجاهلها واضغط موافق ثم اضغط NEXT مرة أخرى



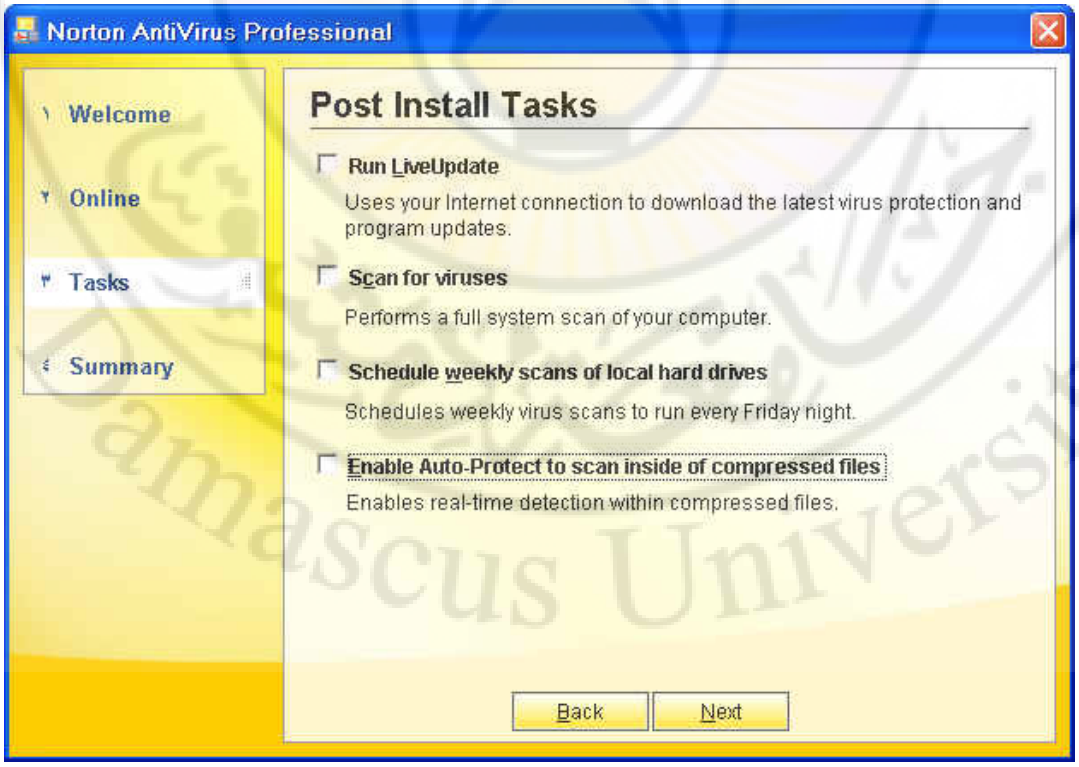
16. اختر Activate my software by phone لتبين أنه تم تسجيل البرنامج عبر الهاتف



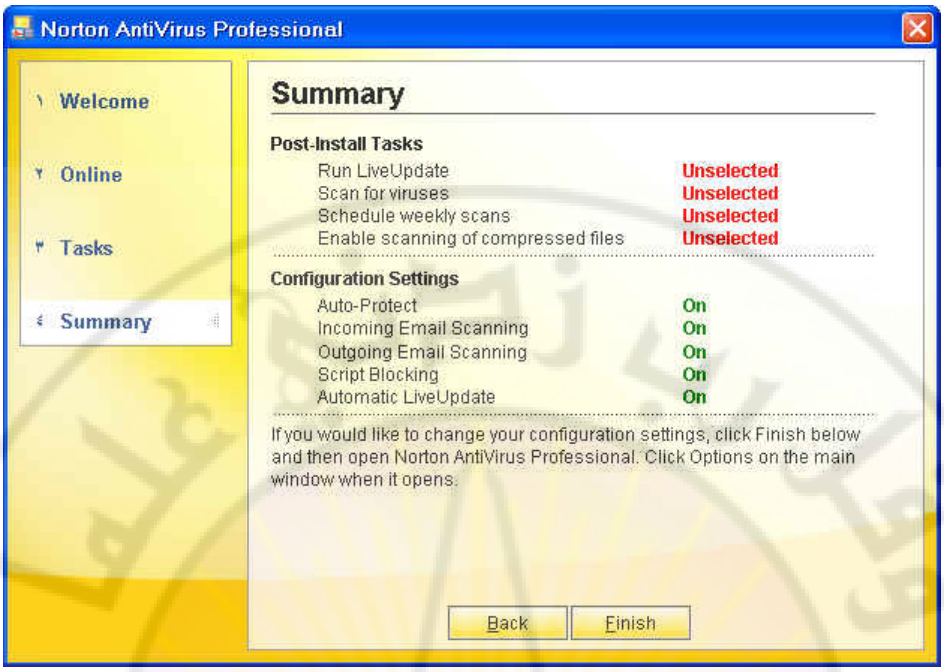
17. في الفقرة الثانية(2) من هذه اللوحة رقم تطلبه الشركة منك لكي تعطيك رقم التسجيل الرئيس(الملكي)، نقوم بوضعه في الخانات الموجودة في الفقرة الثالثة(3)



18. سوف تظهر لك رسالة ACTIVATION SUCCESSFUL أي إنه تم التسجيل بنجاح ثم اضغط NEXT



19. قم بوضع إشارة صح ☑ أمام الخيارات المناسبة أو ألغ العلامة من كل الخيارات، ثم اضغط NEXT



20. اضغط على Finish لإنهاء عملية التسجيل.
21. بعد ذلك أعد تشغيل جهازك حتى يتم حفظ التعديلات.

التمرين الثاني

ضبط إعدادات Norton AntiVirus2004

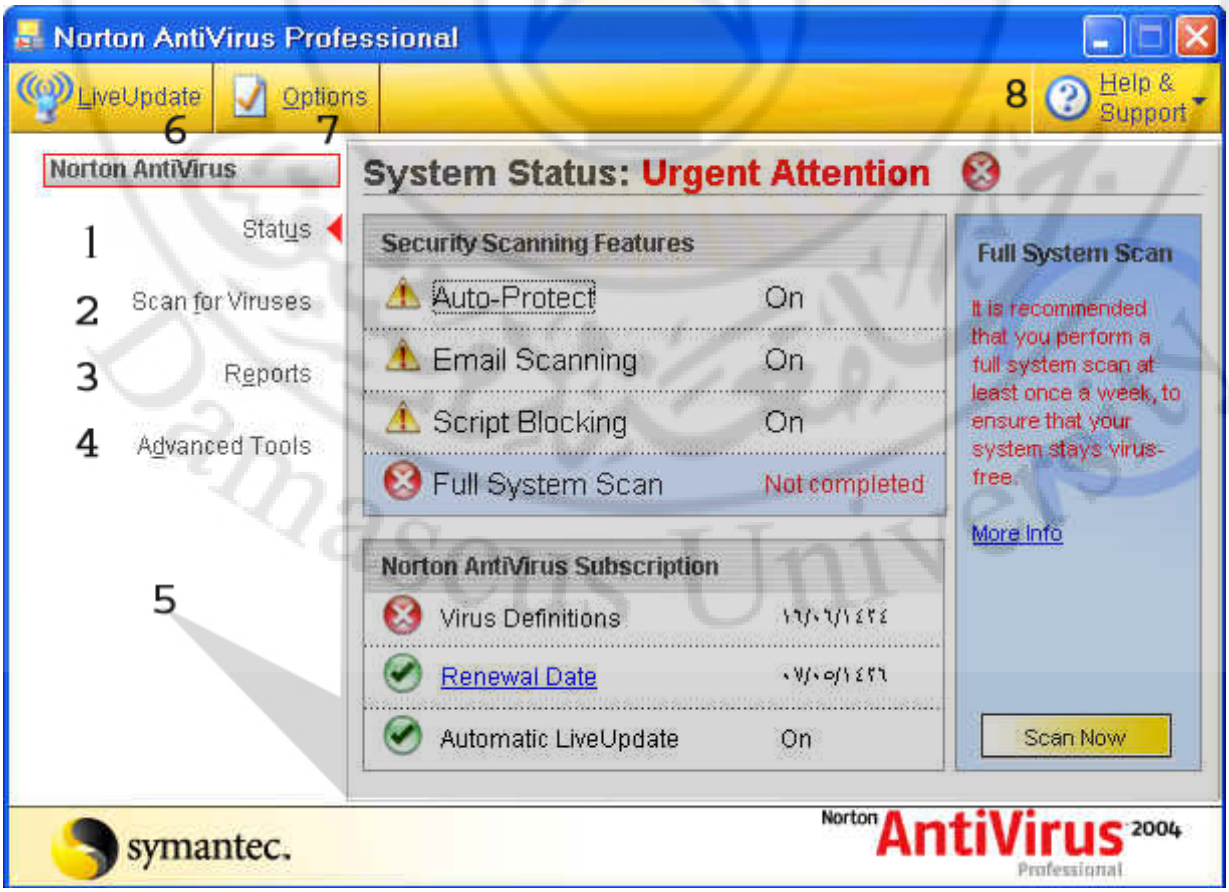
النشاط المطلوب: قم بضبط إعدادات برنامج مكافحة الفايروسات **Norton AntiVirus2004**

الأدوات:

1. قرص برنامج مكافحة الفايروسات Norton AntiVirus2004

الخطوات:

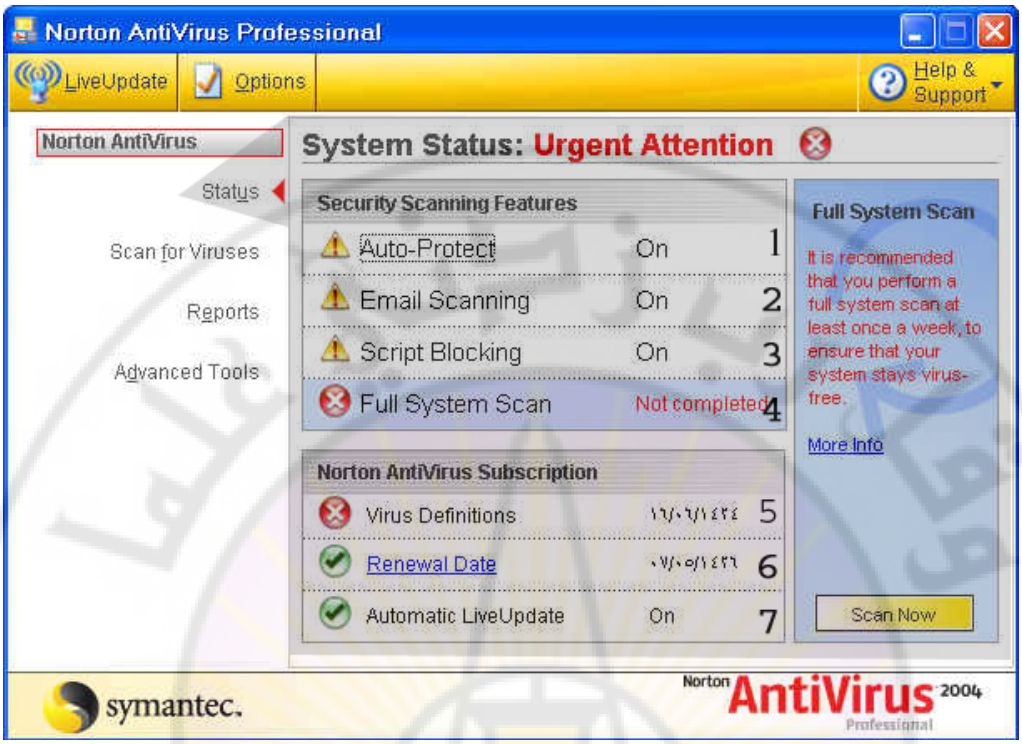
1. قم بتشغيل البرنامج وذلك بالنقر على زر ابدأ ثم البرامج.
2. من قائمة البرامج انقر على Norton Antivirus
3. انقر على أيقونة البرنامج Norton Antivirus2004 Professional
4. ستظهر لك النافذة الرئيسة للبرنامج:



ومن هذه الخيارات تحدد العمل المطلوب، وإليك شرح لكل خيارات هذه الشاشة:.

الرقم	عمل التطبيق	الفائدة
1	يبين حالة اختبار البرنامج للنظام	الفحص الدقيق لـ (الحماية التلقائية، الفحص البريدي، النصوص البرمجية الموجودة بالقائمة السوداء، الفحص الدقيق للقرص الصلب.)
2	الفحص عن الفايروسات	اختيار ما تريد فحصه من القرص الصلب، والأقراص القابلة للإزالة، والأقراص المرنة(جميع موارد التخزين و الملفات على جهاز الحاسب)
3	جمع التقارير	جمع المعلومات عما تم فحصه على جهاز الحاسب و البيانات الكاملة عن الفايروسات و غيرها
4	خيارات متقدمة	لتعديل التغيرات و تنفذ الأوامر المتقدمة المسموح بها
5	عرض التفاصيل	عرض التطبيقات و التفاصيل والخيارات المستخدمة لـ (**الأرقام التوضيحية1،2،3،4**)
6	التحديث التلقائي	لتجنب الفايروسات والنصوص البرمجية المنتشرة حديثاً(الجديدة)
7	الخصائص	تعديل جميع ما تريده من الخيارات الخاصة بالبرنامج وما تريد أن يعمله البرنامج
8	المساعدة	الطريقة الصحيحة في الإرشاد السليم، وتوضيح ما تريده من أي نافذة للبرنامج

5. انقر على Status لتبين حالة اختبار البرنامج للنظام



نجد أنه لم يتم تخطي حالة البرنامج للنظام، وهذا بسبب عدم الفحص الكامل للنظام.

التمرين الثالث

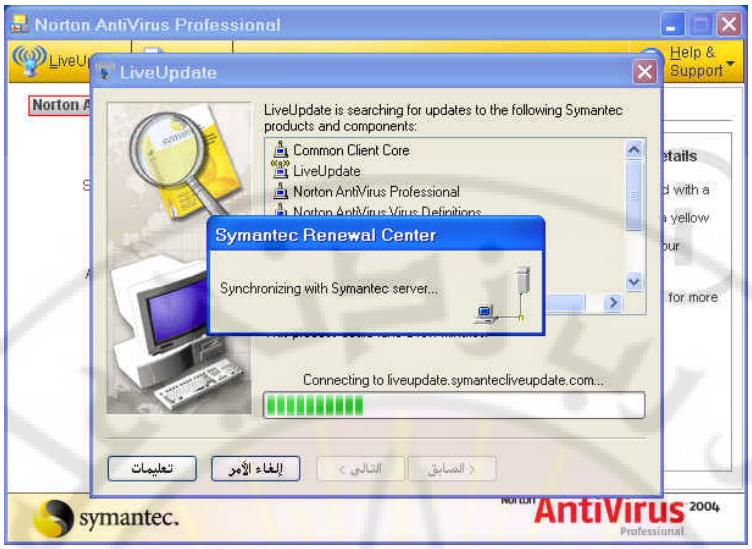
تحديث Norton AntiVirus2004 عبر الإنترنت

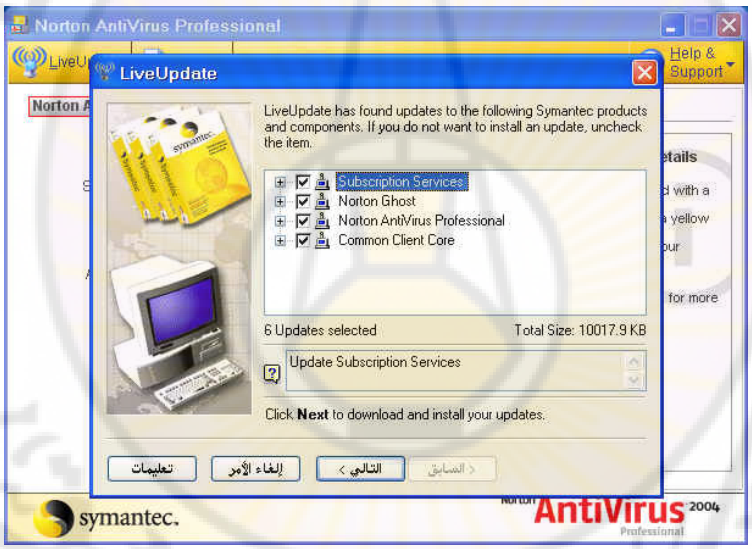
النشاط المطلوب: قم بتحديث برنامج مكافحة الفايروسات **Norton AntiVirus2004** عبر الإنترنت.

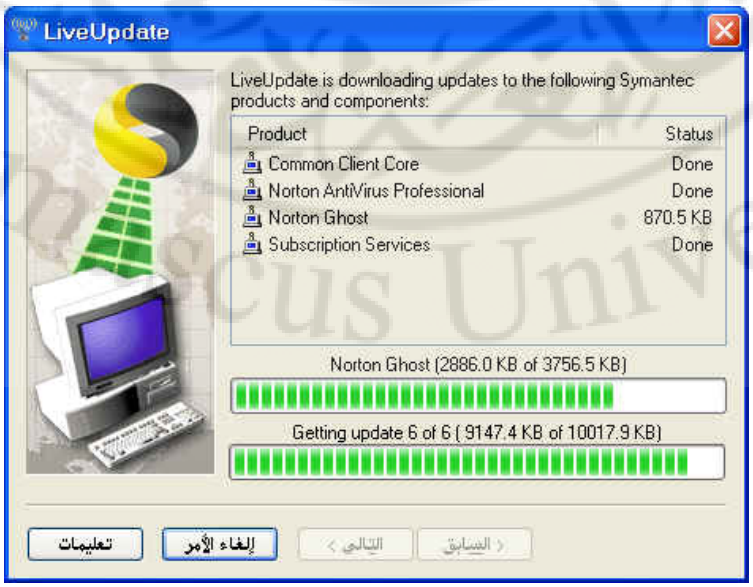
الخطوات:

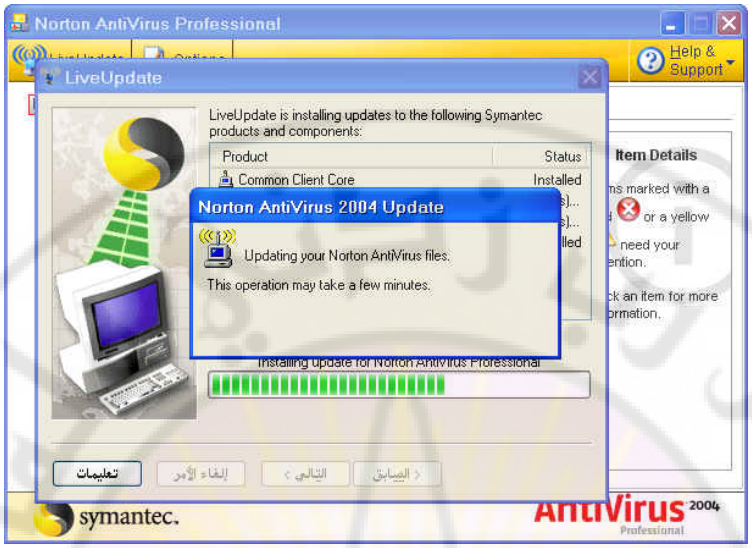
1. قم بتشغيل البرنامج (Norton AntiVirus2004)، ثم انقر على Live Update الموجودة في أعلى النافذة الرئيسة من الجزء الأيسر، ثم انقر على الزر **التالي**

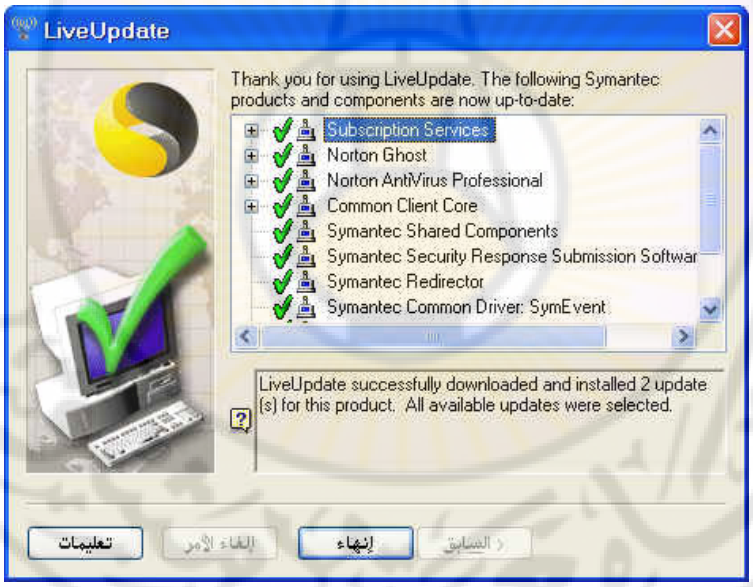
تدل هذه الصورة على الاتصال المباشر للشركة للقيام بعملية التحديث لجميع برامجها الموجودة لجهاز الحاسب


Norton AntiVirus Professional
LiveUpdate
Help & Support
LiveUpdate is searching for updates to the following Symantec products and components:
Common Client Core
LiveUpdate
Norton AntiVirus Professional
Symantec Renewal Center
Synchronizing with Symantec server...
Connecting to liveupdate.symantecliveupdate.com...
تعليمات
إلغاء الأمر
التالي >
< السابق
symantec.
AntiVirus 2004


Norton AntiVirus Professional
LiveUpdate
Help & Support
LiveUpdate has found updates to the following Symantec products and components. If you do not want to install an update, uncheck the item.
Subscription Services
Norton Ghost
Norton AntiVirus Professional
Common Client Core
6 Updates selected
Total Size: 10017.9 KB
Update Subscription Services
Click Next to download and install your updates.
تعليمات
إلغاء الأمر
التالي >
< السابق
symantec.
AntiVirus 2004


LiveUpdate
LiveUpdate is downloading updates to the following Symantec products and components:
Product
Status
Common Client Core
Done
Norton AntiVirus Professional
Done
Norton Ghost
870.5 KB
Subscription Services
Done
Norton Ghost (2886.0 KB of 3756.5 KB)
Getting update 6 of 6 (9147.4 KB of 10017.9 KB)
تعليمات
إلغاء الأمر
التالي >
< السابق


Norton AntiVirus Professional
Help & Support
LiveUpdate
LiveUpdate is installing updates to the following Symantec products and components:
Product
Status
Common Client Core
Installed
Norton AntiVirus 2004 Update
Updating your Norton AntiVirus files.
This operation may take a few minutes.
Installing update for Norton AntiVirus Professional
Item Details
تعليمات
إلغاء الأمر
التالي >
< السابق
symantec.
AntiVirus 2004
Professional


LiveUpdate
Thank you for using LiveUpdate. The following Symantec products and components are now up-to-date:
Subscription Services
Norton Ghost
Norton AntiVirus Professional
Common Client Core
Symantec Shared Components
Symantec Security Response Submission Softwar
Symantec Redirector
Symantec Common Driver: SymEvent
LiveUpdate successfully downloaded and installed 2 update (s) for this product. All available updates were selected.
تعليمات
إلغاء الأمر
إنهاء
< السابق


Restart Required
Some of the updates that were just installed require that you restart your computer now. Please save all unsaved data and then press the OK button to restart your computer.
موافق

التمرين الرابع:

استخدام Norton AntiVirus2004 لتفحص النظام

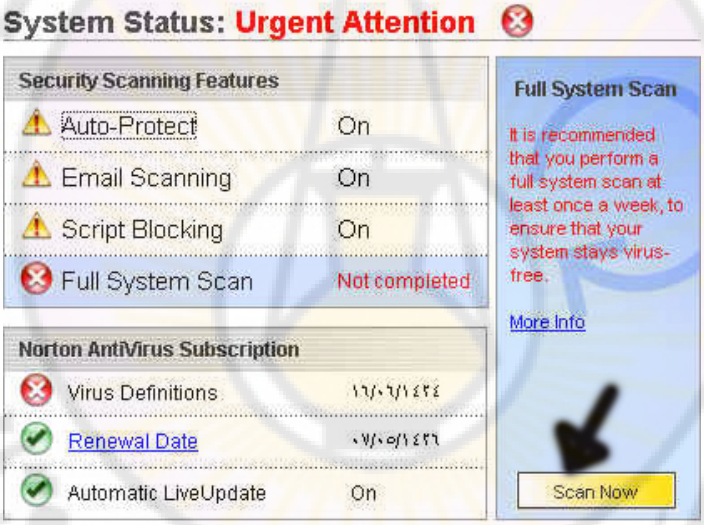
النشاط المطلوب : قم بفحص جهاز الحاسب باستخدام برنامج الحماية من الفايروسات .

الأدوات المطلوبة :

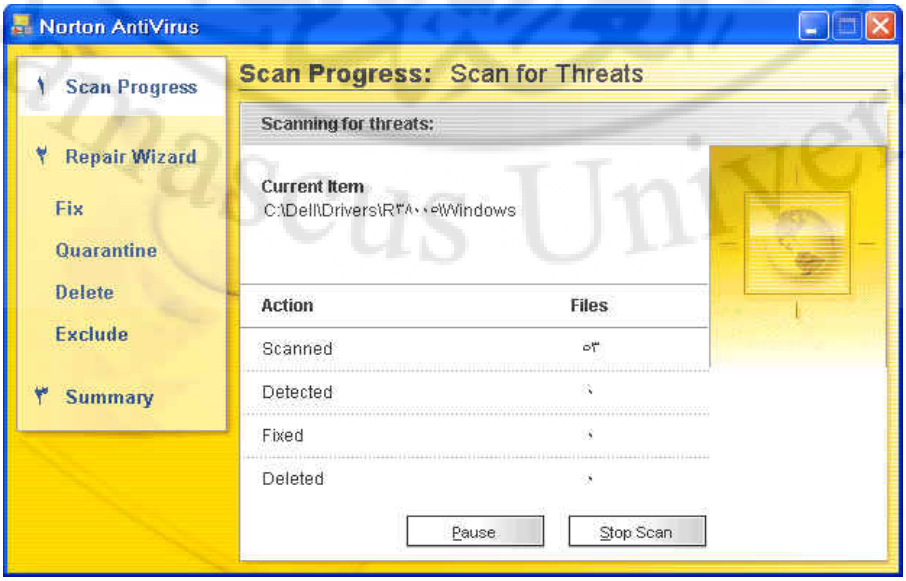
- جهاز حاسب يحتوي برنامج Norton AntiVirus2004 .

خطوات التنفيذ :

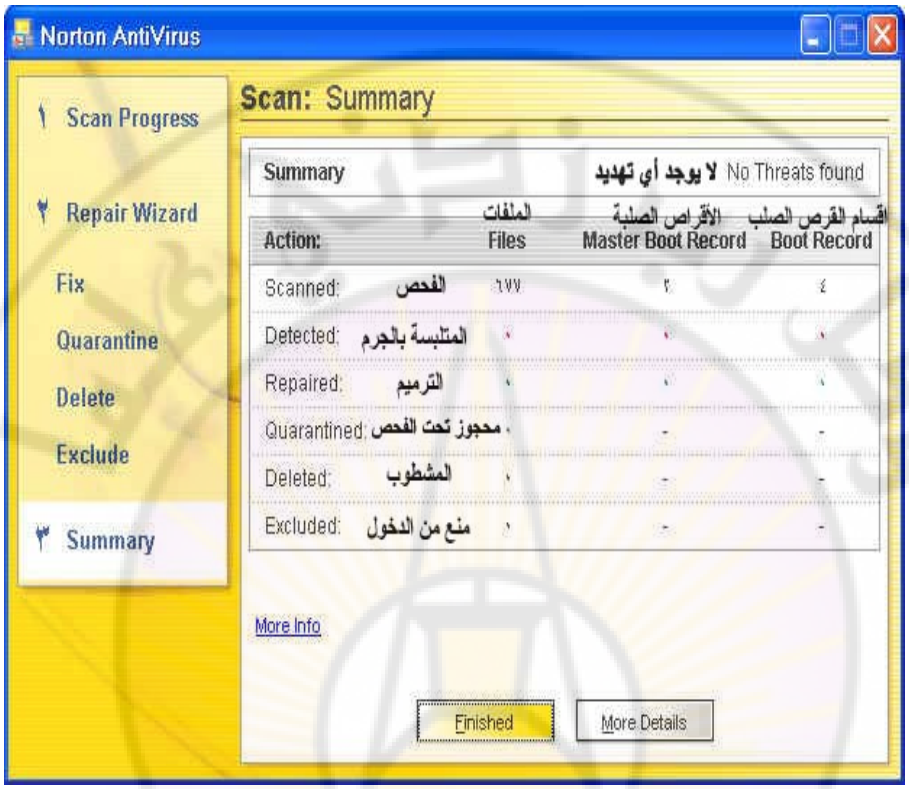
1. قم بتشغيل البرنامج (Norton AntiVirus2004)، ثم انقر على Status الموجودة في النافذة الرئيسة
2. قم بالنقر على Scan Now للقيام بالفحص الكامل للنظام.



ستظهر لك هذه النافذة دلالة على بدء الفحص، انتظر حتى يتم الانتهاء من الفحص الكامل.



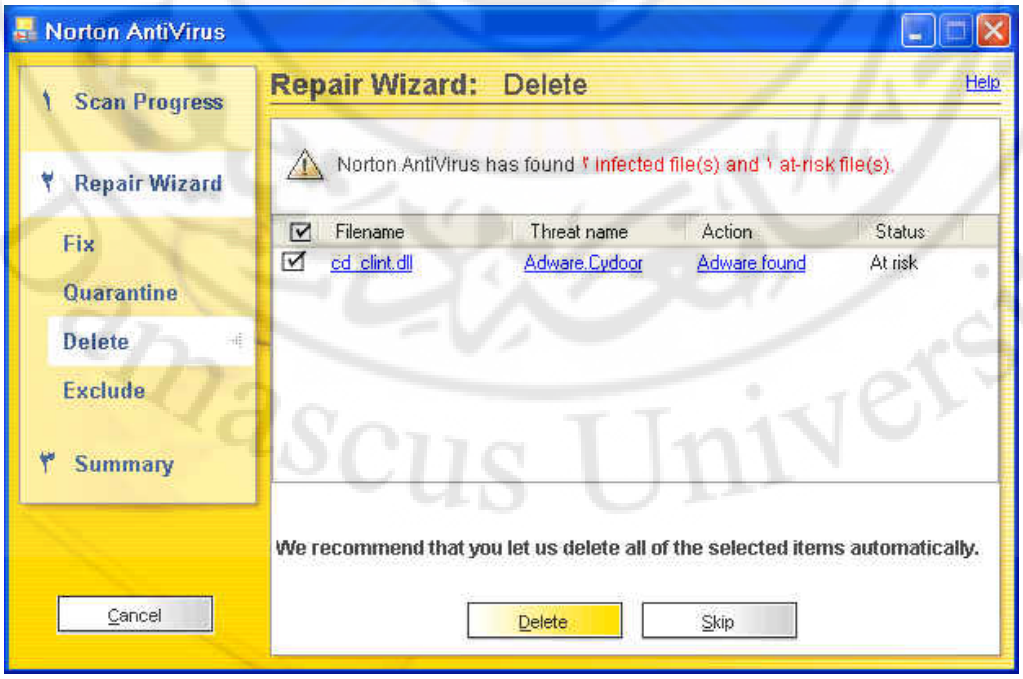
3. هذه النافذة تدلك على الانتهاء من الفحص، دون وجود أي من الفايروسات . انقر على Finished لإغلاق النافذة



أما إذا كان في جهاز الحاسب بعض الفايروسات ستتغير عليك النافذة وتكون :

4. انقر على More Details لمشاهدة التفاصيل

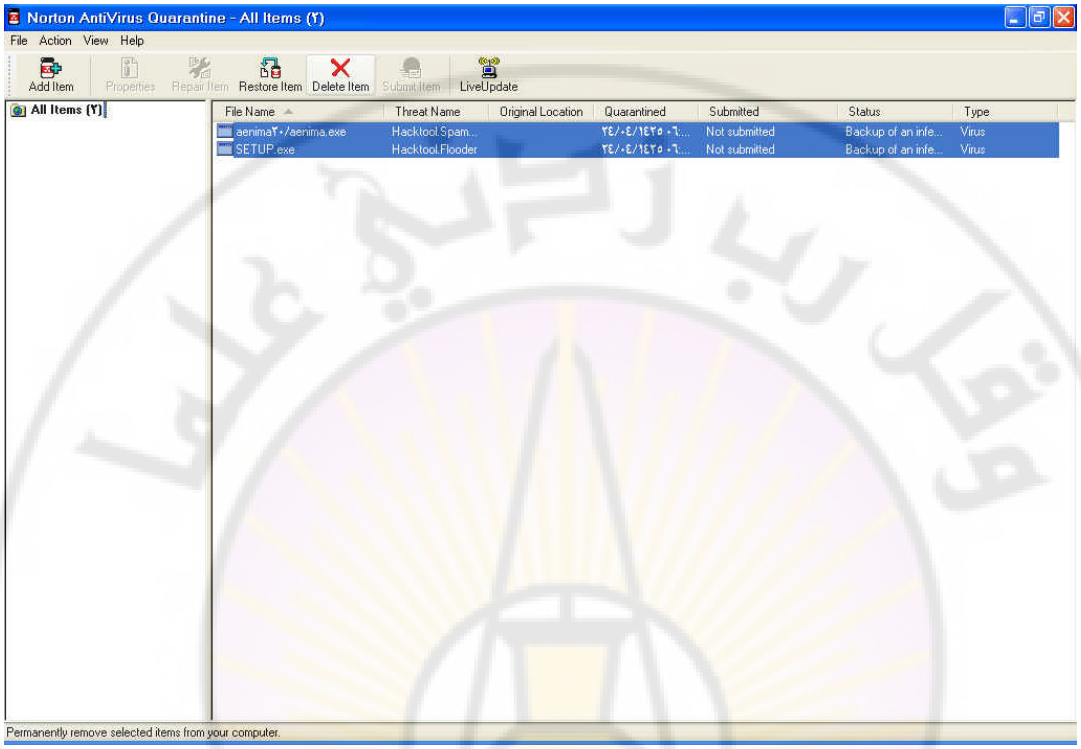
5. لحذف الملف الذي تحت التهديد انقر على Delete في الجزء الأيسر من النافذة



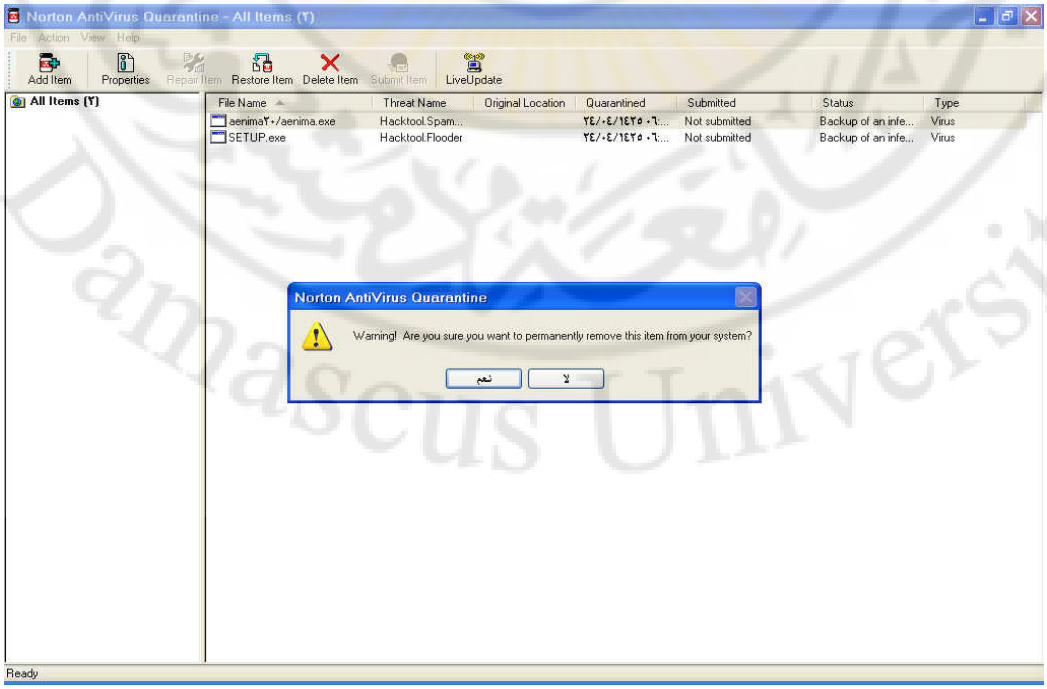
6. ثم انقر على الزر Delete

7. انقر على الزر ☒ في أعلى النافذة من اليمين لإغلاق النافذة

8. انقر على Reports الموجودة في النافذة الرئيسة ، ثم علم على الفايروسات

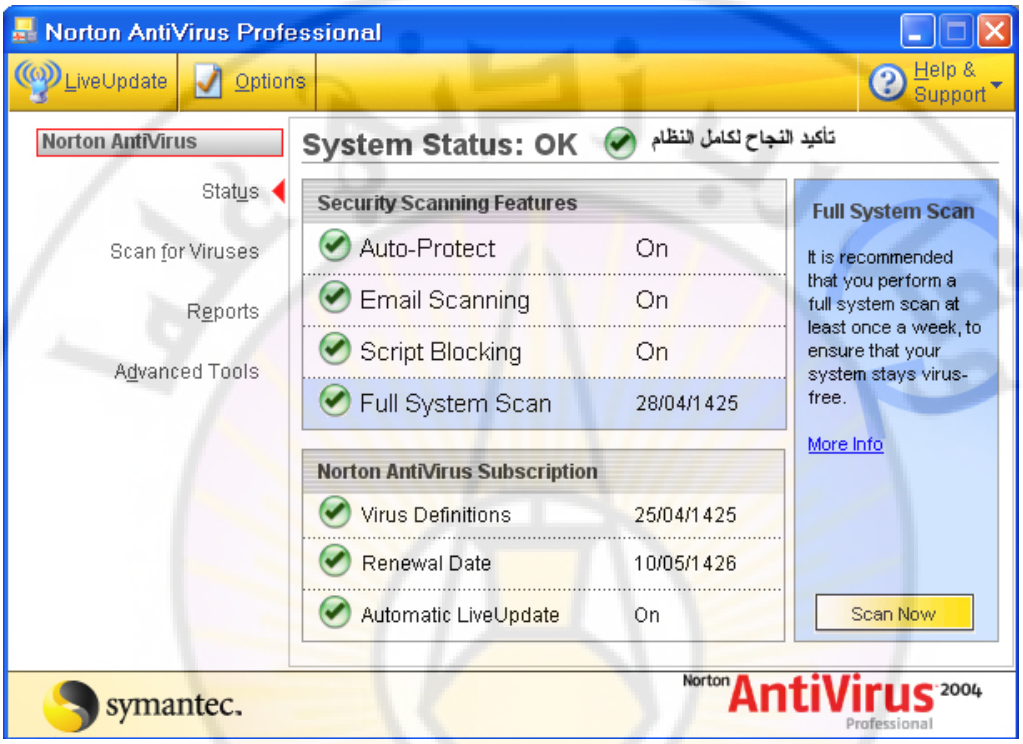


9. انقر على Delete Item لحذف الفايروسات ، ستظهر لك رسالة عن تأكيد الحذف



10. انقر على الزر ☒ في أعلى النافذة من اليمين لإغلاق النافذة

بعد قيامك بالتحديث التلقائي و الفحص(المسح) الكامل لجهاز الحاسب ،ستكون النافذة الرئيسة للبرنامج بهذا الشكل



أسئلة على الوحدة :

س 1- عرف فيروس الحاسب

.....

س 2 – ما هي أعراض الإصابة بالفايروسات ؟

.....

.....

س 3 – ما هي أماكن الإصابة بالفايروسات ؟

.....

.....

س 4 – اذكر بعض أشهر برامج الحماية من الفايروسات

.....

.....

س 5 – ما هي أهم خطوة في تنصيب و إعداد برامج الحماية ؟

.....

تقويم ذاتي

بعد الانتهاء من التدريب على **حماية الجهاز من الفايروسات و الاختراقات** قيم نفسك وقدراتك عن طريق إكمال هذا التقويم لكل عنصر من العناصر المذكورة ، وذلك بوضع علامة (√) أمام مستوى الأداء الذي أتقنته ، وفي حالة عدم قابلية المهمة للتطبيق ضع العلامة في الخانة الخاصة بذلك.

العناصر	مستوى الأداء (هل أتقنت الأداء)			
	غير قابل للتطبيق	لا	جزئياً	كلياً
التعرف على فايروسات الحاسب وأنواعها.				
التعرف على طرق الوقاية من الفايروسات.				
التعرف على أهم برامج الحماية من الفايروسات.				
تركيب برامج الحماية من الفايروسات.				
التعرف على طريقة عمل برامج مكافحة الفايروسات.				

يجب أن تصل النتيجة لجميع العناصر إلى درجة الإتقان الكلي أو أنها غير قابلة للتطبيق ، وفي حالة وجود مفرده في القائمة " لا " أو " جزئياً " فيجب إعادة التدرب على هذا النشاط مرة أخرى بمساعدة المدرب.

تقويم المدرب

معلومات المتدرب	
.....	.....
.....	.....

قيم أداء المتدرب في هذه الوحدة بوضع علامة (√) أمام مستوى أدائه للمهارات المطلوب اكتسابها في هذه الوحدة ويمكن للمدرب إضافة المزيد من العناصر.

	العناصر	مستوى الأداء (هل أتقن المهارة)				
		متقن بتميز	متقن جداً	متقن	متقن جزئياً	غير متقن
1	التعرف على فايروسات الحاسب وأنواعها.					
2	التعرف على طرق الوقاية من الفايروسات.					
3	التعرف على أهم برامج الحماية من الفايروسات.					
4	تركيب برامج الحماية من الفايروسات.					
5	التعرف على طريقة عمل برامج مكافحة الفايروسات.					
6						
7						
8						
9						
10						

يجب أن تصل النتيجة لجميع العناصر إلى درجة الإتقان الكلي أو أنها غير قابلة للتطبيق ، وفي حالة وجود مفرده في القائمة " لا " أو " جزئياً " فيجب إعادة التدرب على هذا النشاط مرة أخرى بمساعدة المدرب.

أقراص التخزين 2

:SCSI(Small Computer System)

SCSI : هي واجهة لربط الأجهزة مع بعضها لتشكيل سلسلة وتعمل بسرعة أكبر من سرعة واجهة ATAتستخدم بشكل أساسي في المخدمات. جميع الأجهزة المتصلة بمأخذ SCSI يمكنها التخاطب مع بعضها بدون الإستعانة بالمعالج ولذلك سمي ب SCSI أي نظام الكمبيوتر الصغير.يمكن وصل أجهزة من أنواع مختلفة CD-ROM, DVD, printer, scanner بشرط أن تدعم تقنية SCSIأي تحوي منفذ خاص بSCSI .الأجهزة التي تدعم الوصل بطريقة SCSI تكون أسرع بالأداء وأغلى سعرا ولذلك يتم إستخدامها في المخدمات بشكل عام حيث يمكن أن تصل سرعتها حتى 320 MBps.

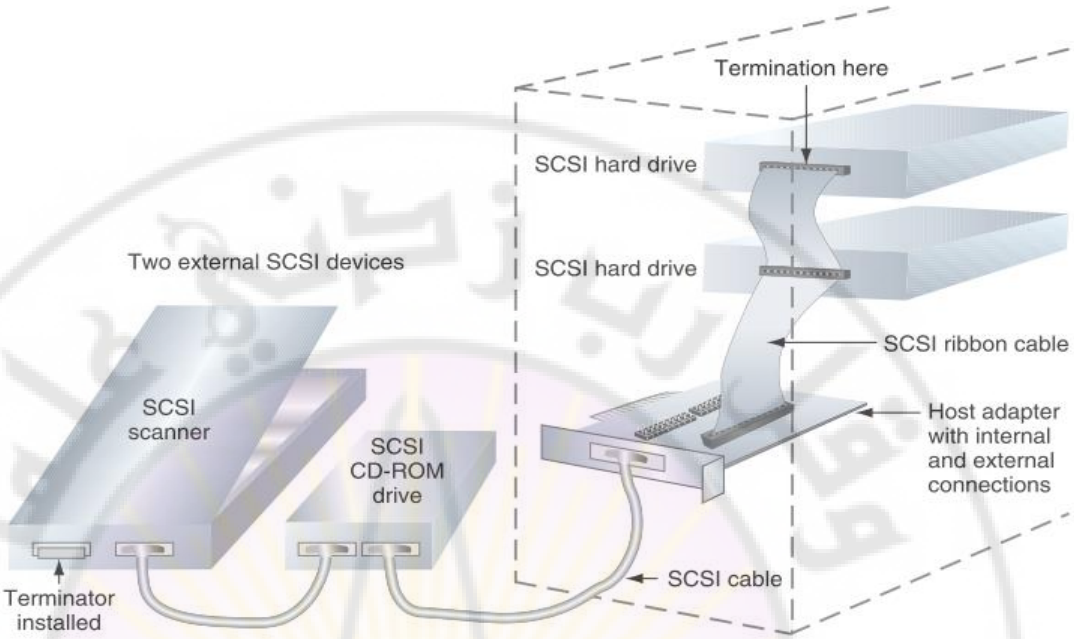
إذا لم تحتوي اللوحة الأم ماخذ خاص بال SCSI يمكن وصل كرت خاص بهذه التقنية يدعى SCSI host adapter card حيث يتم وضعه بمأخذ من نوع PCI ويمكن أن يزود موصلات للأجهزة الداخلية و موصلات للأجهزة الخارجية. سلاسل SCSIهي مجموعة من أجهزة SCSI التي تعمل مع بعضها البعض عبرHost Adapter .

يمكن تقسيم جميع أجهزة SCSI إلى مجموعتين : داخلية وخارجية.

يتم ربط أجهزة ال SCSI الداخلية إلى ال Host Adapter عبر المنفذ الداخلي. أما الأجهزة الخارجية فترتبط بالمنفذ الخارجي لل Host Adapter. ترتبط أجهزة SCSI الداخلية بواسطة كبل يحوي 68 سلكا يؤدي هذا الكبل وظيفة شبيهة تماما بوظيفة كبلPATA .أما الأجهزة الخارجية فترتبط بال Host Adapter بواسطة كبل ذي 50 سلكا عالي الكثافة.

تمتلك معظم أجهزة SCSI الخارجية منفذين أحدهما للارتباط مع متحكم SCSI والثاني للارتباط مع جهاز SCSI آخر لتشكيل سلسلة SCSI خارجية. يمكن أن تحتوي سلسلة SCSI على 15 جهاز كحد أقصى بالإضافة للمتحكم. تستخدم تقنية SCSI معرفات فريدة لهذه الغاية تسميSCSI ID وهو رقم يمكن أن يكون بين 0 و 15 حيث كل جهاز يملك رقم فريد ويتم اعداد هذا الرقم يدويا عند وصل الأجهزة مع بعضها و تطبق قيود الأرقام التعريفية هذه على الأجهزة الموجودة ضمن نفس السلسلة فقط لذلك يمكن أن يمتلك جهازا SCSI نفس الرقم التعريفي طالما أنهما موجودان على سلسلتين مختلفتين.

تستخدم سلاسل الأجهزة الموصولة على كبل SCSI بمايدعى SCSI terminator وهو عبارة عن وصلة توضع بآخر جهاز موصول بالكبل من أجل التخفيف من التشويش الإلكتروني الناتج عن إرتداد الإشارة.



(صورة تظهر صندوق الحاسب و سلسلة SCSI داخلية و خارجية موصولين بكرت SCSI او SCSI Host Adapter وتظهر أين تنتهي كل سلسلة)

- بعد تثبيت القرص بشكل ناجح يجب أن نقوم بخطوتين أساسيتين حتى يستطيع نظام التشغيل التعامل مع القرص الصلب:

1- التقسيم (Partitioning): وهي العملية التي نقوم بها بتقسيم القرص الصلب إلى مجموعة من الاسطوانات Cylinder تدعى Partition أو Volume القرص الصلب يجب أن يملك على الأقل جزء واحد في نظام التشغيل ويندوز كل جزء يسمى بمحرف :C أو :D ...الخ.

2- بعد عملية التقسيم يجيب تهيئة القرص Format وهي عملية تنصيب نظام الملفات على الجزء وذلك من أجل تنظيم القرص بطريقة تمكن نظام التشغيل من تخزين الملفات والمجلدات وعلى هذا الجزء واسترجاعها وهناك عدة أنواع من أنظمة الملفات سوف نتحدث عنها فيما بعد .

- تدعم إصدارات ويندوز windows 7 ,vista, 2000/xp طريقتين لتقطيع محركات الأقراص:

1-التقطيع حسب سجل الإقلاع الرئيسي Master Boot Record

2- التقطيع بطريقة التخزين الديناميكي Dynamic Storage وهي مملوكة من شركة Microsoft حصريا.

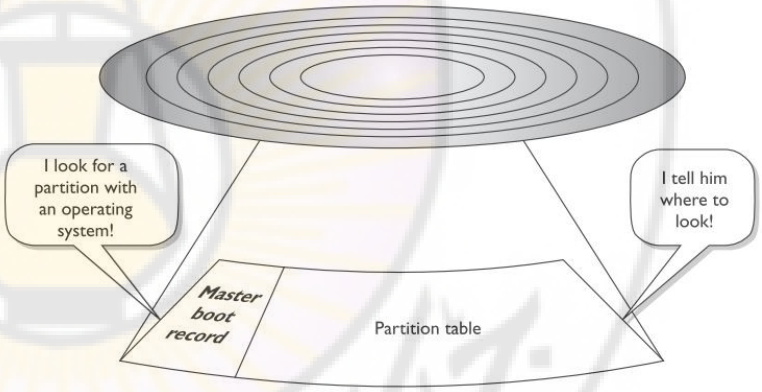
الأقراص المقطعة حسب MBR تدعى أقراص أساسية (Basic Disks)أما الأقراص المقطعة حسب التخزين الديناميكي فتدعى الأقراص الديناميكية (Dynamic Disks)

- عند التقطيع وفق طريقة MBR يتم انشاء منطقتين من البيانات في محرك الأقراص تخزن في boot sector ببداية القرص الصلب:

1- سجل الإقلاع الرئيسي MBR اختصارا ل Master Boot Record

2- جدول التقطيع Partition Table

كما نرى في الشكل التالي:



- سجل الإقلاع الرئيسي MBR: هو قطعة صغيرة من الشيفرة البرمجية التي تسيطر على عملية الإقلاع بعد أن ينتهي نظام Bios من عمله ويتوضع على قطاع الإقلاع الرئيس Boot Sector المتوضع في platter1, side 0, Track 0, Sector 1 من القرص .مهمة MBR هو أن يبحث ضمن جدول التقطيع Partition Table عن جزء محرك الأقراص الذي يحوي نظام تشغيل قابل للإقلاع.

- جدول التقطيع (Partition table): يحوي معلومات عن كل جزء على القرص الصلب مثلا الجزء الذي يحوي نظام التشغيل (Active) وعنوان بداية كل جزء على القرص الصلب.

- يدعم جدول التقطيع(Partition table) الموجود ضمن الأقراص الأساسية (Basic disks) نوعين من التقطيعات :

1- الأقسام الأولية Primary partition: الأجزاء الأولية مصممة لدعم انظمة التشغيل القابلة للإقلاع أما الأجزاء الموسعة فلايمكن الإقلاع منها.

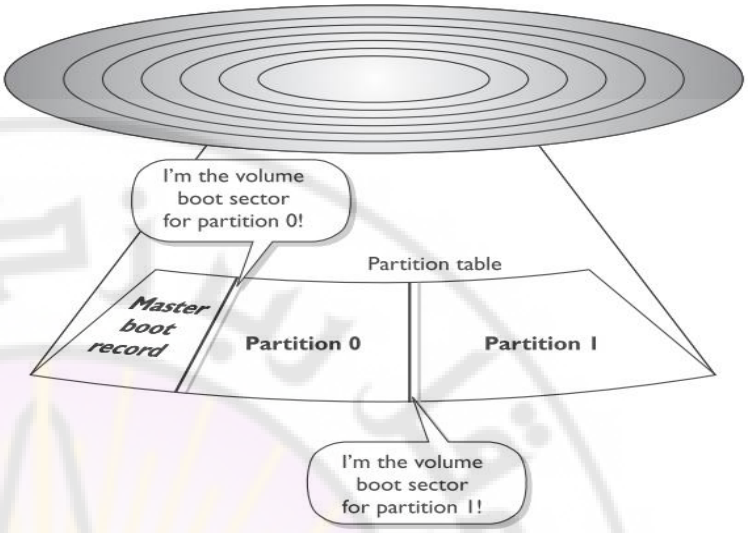
2- القسم الموسع Extended partition:

القسم الموسع ليس ضروريا حتى نباشر العمل على نظام التشغيل و القرص الصلب فيمكن أن نستخدم قرص صلب مقسم كأربع أقسام أولية فقط أو قسم أولي كبير ولكن إذا أردنا عدد كبير من الأقسام فيجب استخدام الأقسام الموسعة.

- يمكن أن يحتوي القرص الأساسي على ثلاثة تقطيعات أولية كحد أقصى وجزء موسع واحد فقط.
- إذا لم يوجد جزء موسع في محرك الأقراص الصلبة لديك فيمكن أن تنشيء اربع أجزاء أولية كحد أقصى ويمكن وقتها تنصيب أربع أنظمة تشغيل كحد أقصى على الحاسب واختيار نظام التشغيل الذي نريد العمل معه عند اقلاع الحاسب.
- بالعادة الجزء الموسع لا يأخذ محرف خاص به ويجب بعد إنشاء جزء موسع أن ننشئ أقراص منطقية Logical Drives وتحصل على أحرف ضمن D حتى Z ويمكن انشاء العدد الذي نرغب به من الأقراص المنطقية ضمن هذا الجزء الموسع. الحرف :C محجوز لأول قسم أولي الذي يتوضع عليه نظام التشغيل في نظام ويندوز .
- يمتلك كل جزء أولي(primary partition) على محرك أقراص واحد إعدادا خاصا يسمى Active أو مفعل يتم تخزينه ضمن جدول التقطيع Partition Table .يكون هذا الإعداد إما ممكنا Enable أو غير ممكن Disable من أجل كل جزء أولي. وهذه الخاصية تساعد ال MBR في تحديد أي قرص أولي يحوي نظام التشغيل المراد تحميله و إعطاء التحكم له .

  - ملاحظة : لأننا لايمكن أن نقلع سوى من نظام تشغيل واحد في الوقت الواحد فإننا يمكن أن نملك جزء أولي واحد كجزء Active.

- قطاع الإقلاع boot sector المتواجد ببداية القرص الصلب ليس القطاع الوحيد الخاص حيث هناك قطاع خاص آخر يتواجد في القطاع الأول من الاسطوانة الأولى الخاصة بجزء معين يدعى volume boot sector ومهمته تخزين معلومات خاصة بالجزء مثل مكان تواجد ملفات الإقلاع المتواجدة على هذا الجزء و حجم الجزء ...الخ. كما يظهر لدينا بالشكل لدينا جزأين فقط يحوي كل جزء ببدايته volume boot sector.



تقطيعات أخرى :

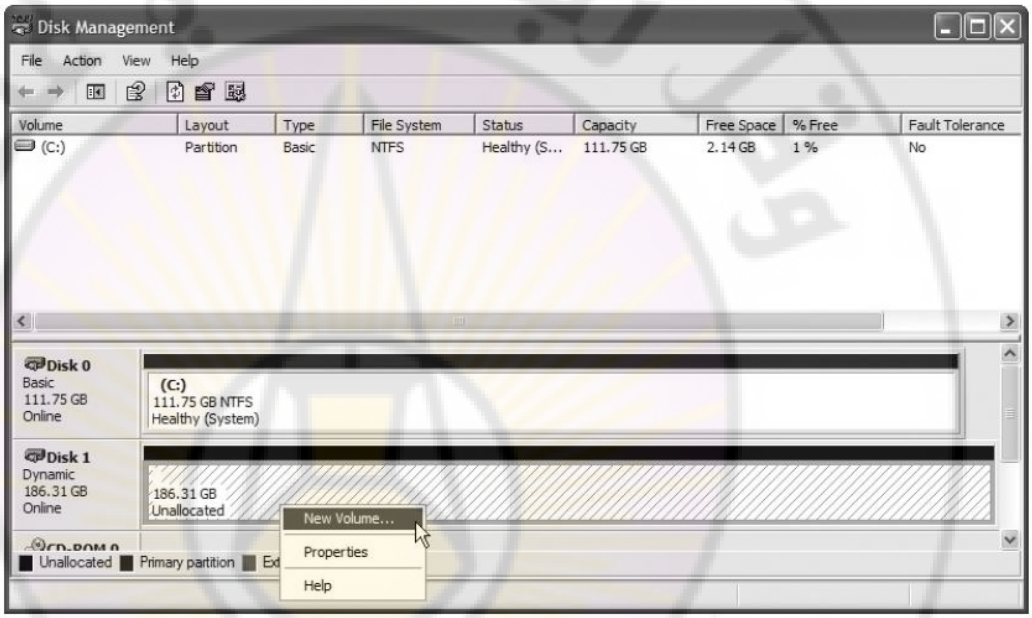
Page file: هو عبارة عن ملف مخصص ليعمل على شكل ذاكرة RAM إضافية عندما يحتاج النظام لكمية من الذاكرة أكثر مما هو متوفر لديه وهي خاصة بنظام التشغيل ويندوز ويدعى Swap file أو ملف الصفحات Page file وهو عبارة عن ملف وليس جزء كامل من محرك الأقراص أما في أنظمة لينكس فاسمه Swap partition ويكون على شكل جزء كامل وليس ملف كما في نظام التشغيل ويندوز يمكن أن نراه على القرص c:\ بإسم pagefile.sys وذلك بعد اظهار الملفات المخفية وملفات النظام من خيارات المجلد.

الأقراص الديناميكية : Dynamic Disks

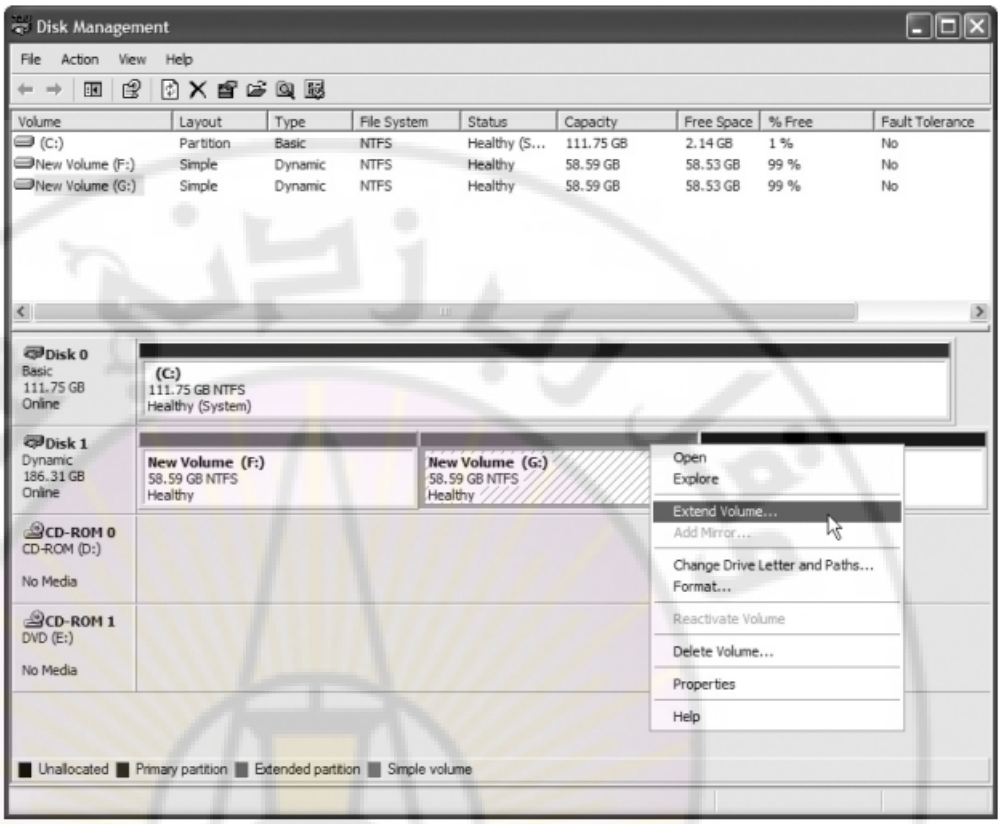
- تم طرحها مع وصول ويندوز 2000
- تخلت الأقراص الحيوية عن الإصطلاح Partition و استخدمت عوضا عنه الإصطلاح Volume.
- لايوجد ضمن مفهوم الأقراص الحيوية مايكافيء الأجزاء الأولية والموسعة.
- يتم تحويل قرص من Basic إلى Dynamic بإستخدام أداة ويندوز Disk Management وذلك بالنقر بالزر اليميني على القرص الصلب المثبت واختيار تحويل إلى Dynamic ولكن لا يمكن التحويل بالعكس بدون فقد جميع البيانات.
- يتم التحويل إلى قرص ديناميكي من أجل الاستفادة من الخصائص التي تدعمها الأقراص الديناميكية كأنواع الأقراص التي سوف نراها مثل simple volume, stripped volume....إلخ.

■ تستطيع الأقراص الحيوية إنشاء خمسة أنواع لل Volume وذلك باستخدام أداة ويندوز Disk Management :

1- Simple Volume: تعمل بشكل شبيه للأجزاء الأولية Primary فإذا كان لدينا محرك ألأقراص صلبة واردنا أن نجعل نصفه قرص c والنصف الآخر قرص D فسنقوم بإنشاء حجمين ضمن قرص حيوي ولا توجد حاجة لإنشاء جزء أولي وجزء موسع.

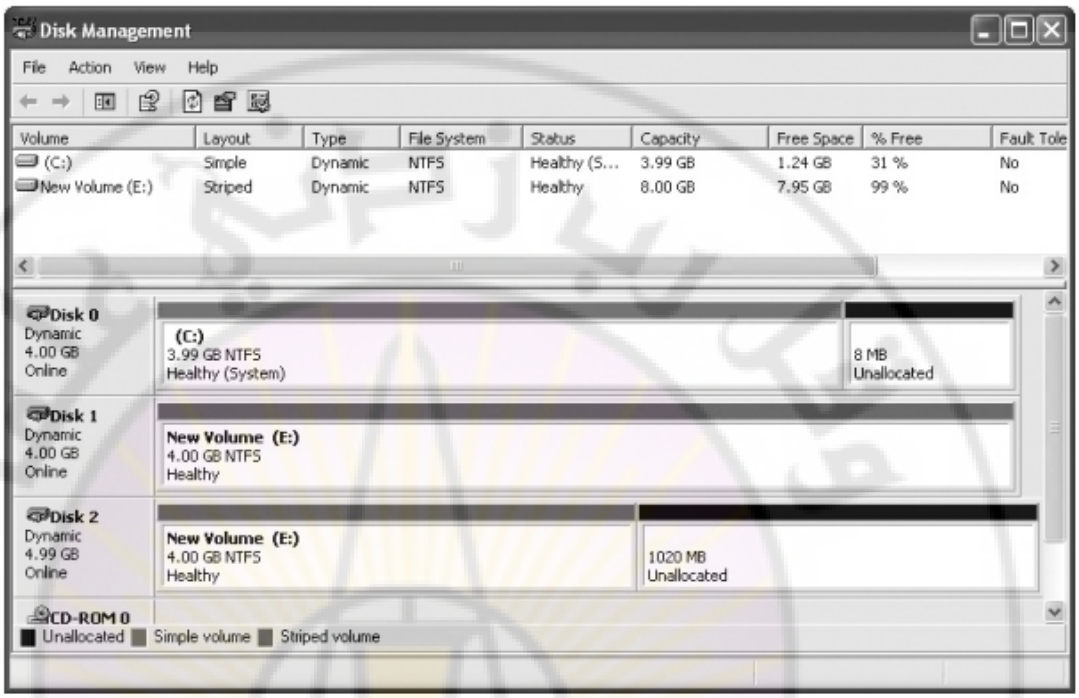


2- Spanned volume: تستخدم من أجل تمديد مساحة قرص وذلك بأخذ مساحة غير مخصصة من أقراص أخرى unallocated يمكن تنفيذ ذلك باختيار القرص الديناميكي بالزر اليمين واختيار Extend volume و اختيار الأقراص والمساحة المراد تمديدها . في حال بدأت المساحة تنفذ على القرص الصلب المركب يمكن تركيب قرص صلب آخر من نوع ديناميكي و تمديد مساحة القرص الأول عليه وبذلك تبقى الملفات على القرص الأول و المحرف الخاص بالقرص الأول مثلا c: .



3- Striped volume: نستطيع باستخدام هذا النوع من الأقراص الديناميكية دمج مساحتين غير مخصصتين على محركي أقراص صلبة مختلفين لتجعل منهما Volume واحد حيث يتم كتابة وقراءة أي ملف وتوزيعة على القرصين على التوازي ويستخدم بذلك محركي أقراص بدلا من محرك واحد مما يسرع من عملية القراءة والكتابة . ولكن أيضا مشكلته أنه أيضا إذا تعطل أحد الأقراص فسيتم فقدان كافة البيانات. يشترط بالمساحة الغير مخصصة على القرصين أن تكونا متساويتين .

كما يظهر من الشكل لدينا Disk 1 و Disk 2 من نوع Striped volume وكل منهما يستخدم مساحة 4 GB.



4- Mirrored volume: هي تشكيل RAID 1 ستأخذ مساحتين غير مخصصتين (Unallocated)على محركي أقراص صلبة مختلفين وتجعل إحداهما مرآة للأخرى أي أن البيانات التي يتم نسخها على القرص تنسخ أيضا على القرص الثاني كنسخة احتياطية.إذا تعطل أحد محركي الأقراص المشكلين بهذه الطريقة فسيبقى الآخر على قيد العمل توجد في windows server فقط .

5- RAID 5 volume: وهي كما يدل إسمها تشكيل RAID 5 .يحتاج هذا التشكيل إلى ثلاثة محركات أقراص على الأقل وتحتوي كل منها على نفس القياس من المساحة غير المخصصة (Unallocated)توجد في windows server فقط .

ملاحظة : الحجوم RAID 5 و Mirrored لا توجد إلا في المخدمات servers لذلك لانراها في إصدارات ويندوز العادية مثل XP professional أو Windows 7.

عند وصل أي قرص صلب بالحاسب وفتحنا على الأداة Disk Management في ويندوز فإننا نرى الحالات التالية للقرص :

- Healthy: تعني أن القرص بحالة سليمة ويعمل بشكل جيد.
- Unallocated: تظهر عندما يكون القرص غير مقطع.
- Foreign drive: نرى هذه الحالة عند نقل قرص حيوي Dynamic من حاسب لآخر.
- Formatting: كما هو واضح تظهر هذه الحالة عندما يكون القرص في حالة تهيئة.
- Failed: تظهر عندما يكون القرص عاطل ولايمكن إصلاحه.
- Online: عندما يكون القرص متصل بشكل صحيح بالحاسب.
- Offline: يكون القرص إما عاطل أو غير متصل بشكل صحيح بالحاسب.

أنظمة الملفات ضمن نظام ويندوز

يأتي كل إصدار لنظام ويندوز مزودا بأداة تهيئة تسمح بإنشاء نوع واحد أو أكثر من أنظمة الملفات على أحد الأجزاء أو الحجوم. إصدارات ويندوز قيد الاستخدام حاليا قادرة على التعامل مع ثلاثة أنظمة مختلفة للملفات :
FAT16,FAT32,NTFS

وحدة التخزين الأساسية ضمن محرك الأقراص الصلبة هي القطاع . يستطيع كل قطاع تخزين 512 بايت من البيانات كحد أقصى. إذا تم تخزين ملف قياسه أقل من 512 بايتا ضمن أحد القطاعات فستضيع مساحة التخزين المتبقية ضمن ذلك القطاع. نحن نقبل بنسبة الضياع هذه لأن معظم الملفات تكون بقياس أكبر بكثير من 512 بايت. إذا ما الذي يحدث عندما يتم تخزين ملف قياسه أكبر من 512 بايت ؟ يحتاج نظام التشغيل لطريقة لملء قطاع واحد ومن ثم العثور على قطاع آخر غير مستخدم ليتابع ملأه إلى أن يتم تخزين كامل الملف. عند الانتهاء من تخزين كامل الملف يجب أن يتذكر نظام التشغيل القطاعات التي قام بتخزين الملف عليها حتى يتمكن من استرجاعه فيما بعد.

- تشابه بنية FAT جدولا بعمودين يتم ترقيم العمود اليساري بأرقام القطاعات من 0000 إلى FFFF بالنظام الست عشري يعني ذلك أنه يوجد 65,536 قطاع حيث نلاحظ أن العمود اليساري يحتوي على 16 بت أما العمود اليميني فيحتوي على معلومات حول القطاع
- إذا لم يكن من الممكن القراءة من أحد القطاعات فسيتم تخزين رمز حالة خاص FFF7 ضمن موقع القطاع في بنية FAT يشير إلى أن هذا القطاع غير متوفر للاستخدام. يتم ايضا تخزين رمز الحالة 0000 للإشارة إلى أن القطاع الموافق قابل للإستخدام.

0000	
0001	
0002	
0003	
0004	
0005	
0006	
FFF9	
FFFA	
FFFB	
FFFC	
FFFD	
FFFF	
FFFF	

- لايستطيع جدول FAT16 سوى عنونة 2^{16}x512=32 MB

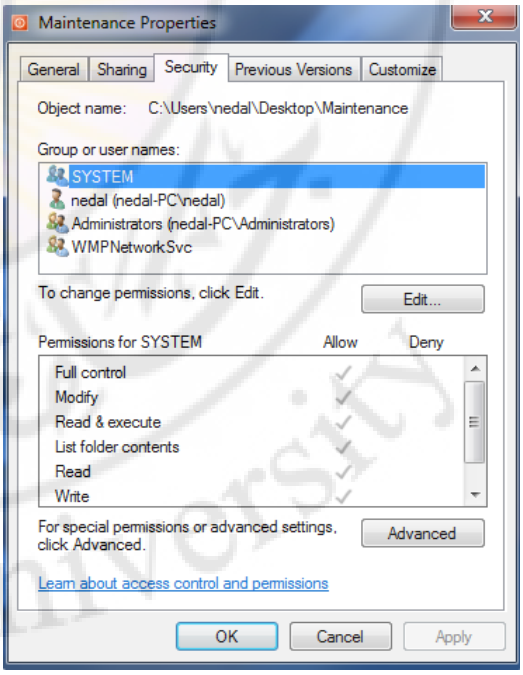
- تم تطوير نظام الملفات FAT16 بإستخدام فكرة العناقيد Clusters والتي تعني تجميع عدد من القطاعات المتجاورة ومعاملتها كوحدة منفردة ضمن نظام ال FAT حيث أصبح كل سطر في جدول ال FAT يعنون عنقودا كاملا عوضا عن قطاع واحد
- لا تكون العناقيد ثابتة بل يمكن تغير قياسها عند التهيئة حسب الحاجة لكن هذا النظام استمر في دعم 2^{16} وحدة تخزين فقط لذا يتم تحديد قياس العنقود (أي عدد القطاعات المحتواة فيه) أثناء عملية التهيئة حسب القياس الكلي للجزء.
- قد اصبح نظام FAT16 الجديد يدعم سعات تصل إلى 2 جيجابايت كحد أعظمي لمحركات الأقراص الصلبة.
- يدعم نظام FAT32 أجزاء من محركات الأقراص الصلبة بسعة عظمى تصل إلى 2 تيرابايت
- يستخدم نظام FAT32 32 بت لوصف كل عنقود مما يعني أنه يمكن تخفيف قياس العناقيد إلى قيم معقولة .
- لو كان لدينا جزء قرص صلب بقياس 2 جيجا بايت مهيأ حسب نظام FAT16 لكان قياس كل عنقود فيه يبلغ 32 كيلوبايت بينما لو تمت تهيئة نفس الجزء بإستخدام نظام FAT32 لأصبح قياس العنقود فيه 4 كيلوبايت فقط.

- يستخدم نظام الملفات NTFS العناقيد وجداول تخصيص الملفات لكن بطريقة أكثر تعقيدا وأكثر قوة مقارنة مع نظامي FAT16, FAT32 يوفر نظام NTFS ستة تحسينات وميزات إضافية :

- 1- الأمن (Security)
- 2- الضغط (Compression)
- 3-التشفير (Encryption)
- 4- حصص الأقراص(Disk Quotas)
- 5- قياس العناقيد (Cluster Sizing)

نظام NTFS- الأمن (security)

- يتعامل نظام NTFS مع الملفات والمجلدات على أنها أغراض ويوفر مستوى من الأمن لها عبر ميزة تسمى قائمة التحكم بالوصول (ACL أو Access Control List) حيث يمكن لمسؤول الحاسب بإعداد خيارات الوصول لملف أو مجلد معين عن طريقة الضغط بالزر اليمين و اختيار البند Security وإختيار السماحيات حسب المستخدمين مثل سماحية القراءة والكتابة و التنفيذ كما نرى في الشكل التالي :



نظام NTFS- الضغط(Compression)

- يسمح نظام NTFS بضغط الملفات والمجلدات لتوفير مساحة تخزين إضافية على القرص الصلب .

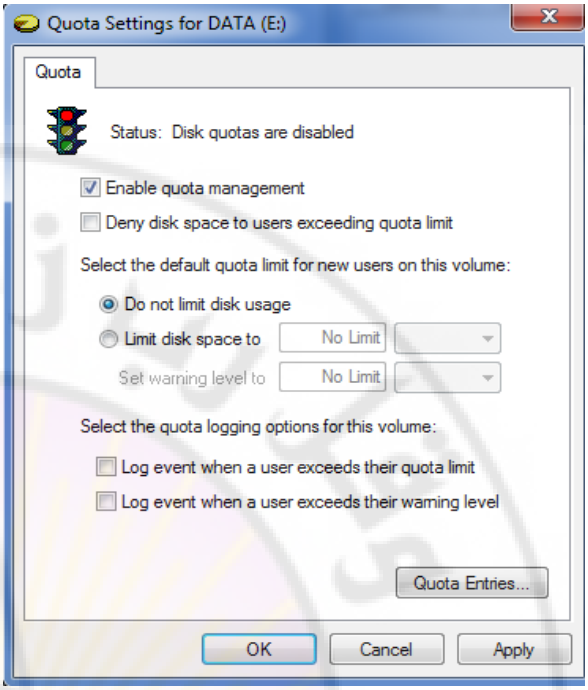
- سيؤدي ضغط الملفات إلى زيادة زمن الوصول إلى البيانات لأن نظام التشغيل سيضطر في هذه الحالة على فك ضغط الملفات أولا في كل مرة يطلب فيها المستخدم التعامل معها. لكن إذا كانت مساحة التخزين المتوفرة لديك محدودة فقد يكون ذلك هو الحل الوحيد أمامك.
- الملفات التي يتم ضغطها بالعادة يتغير لونها لتصبح باللون الأزرق.

نظام NTFS- التشفير(Encryption)

- إحدى أكبر الميزات التي تم تزويد نظام الملفات NTFS بها هي القدرة على تشفير الملفات أي جعلها غير مقروءة لاي شخص لايملك مفتاح فك التشفير المناسب.
- تستطيع تشفير ملف واحد أو مجلد كامل مليء بالملفات
- تطلق شركة ميكروسوفت على خدمة التشفير ضمن نظام NTFS اسم نظام تشفير الملفات (EFS أو Encryption File System)
- لكي نقوم بتشفير ملف أو مجلد يمكن النقر بالزر اليمين واختيار Properties ثم Advanced واختيار Encrypt contents to secure data
- عند تشفير الملفات يتغير لونها ليصبح باللون الأخضر .
- لايؤدي تشفير الملف إلى اخفائه بل يجعله غير قابل للقراءة من قبل المستخدمين الآخرين

نظام NTFS- حصص الأقراص(Disk Quotas)

- يدعم نظام NTFS ميزة حصص الأقراص (Disk Quotas) ممايسمح لمدراء النظام بتحديد قيمة عظمى من مساحة التخزين المسموح بها لكل مستخدم.
- لتحديد الحصص يجب أن تسجل دخولك على حساب يتمتع بصلاحيات المدير ومن ثم تنقر باليمين على القرص الصلب المطلوب وتحدد البند خصائص properties من القائمة ضمن صندوق حوار خصائص القرص ننتقل إلى البند Quota ونقوم بإجراء التعديلات المطلوبة .
- رغم أنه من النادر استخدام هذه الميزة ضمن الانظمة وحيدة المستخدمم إلا أنها ذات أهمية كبيرة ضمنت الأنظمة متعددة المستخدمين لأنها تمنع أحد المستخدمين من احتكار مساحة التخزين المتوفرة لنفسه.



نظام NTFS- قياسات العناقيد(Cluster sizing)

- على عكس نظامي FAT16, FAT32 يسمح نظام NTFS بتعديل قياس العناقيد على سطح القرص الصلب على الرغم من أنك نادرا ماستقوم بذلك
- بشكل افتراضي يدعم نظام NTFS اجزاء محرك الأقراص الصلبة بسعة عظمى تصل إلى 16 تيرابايت على الأقراص الحيوية لكن إذا غيرت من قياس العناقيد فقد تستطيع جعل نظام NTFS يدعم أجزاء تصل سعتها إلى 16 إكسابايت أي 2^{64}

أقراص التخزين

Storage Devices

مكونات القرص الصلب الفيزيائية :

1-(المحور)Spindle:

وهو عبارة عن محور يتركز حوله الأقراص platters ويقوم بتحريكها بشكل دائري وتقاس سرعته ب RPM(Rotation Per Minute)دورة بالدقيقة

2-(الأقراص)Platters:

وهي عبارة عن أقراص فيزيائية مصنوعة من مادة الألمنيوم الخفيف المطلية بمادة مغناطيسية رقيقة تتوضع داخل القرص الصلب و يخزن عليها البيانات بطريقة مغناطيسية. كل Hardisk يحتوي على قرص أو أكثر .

3-(رؤوس القراءة والكتابة)Read/Write head:

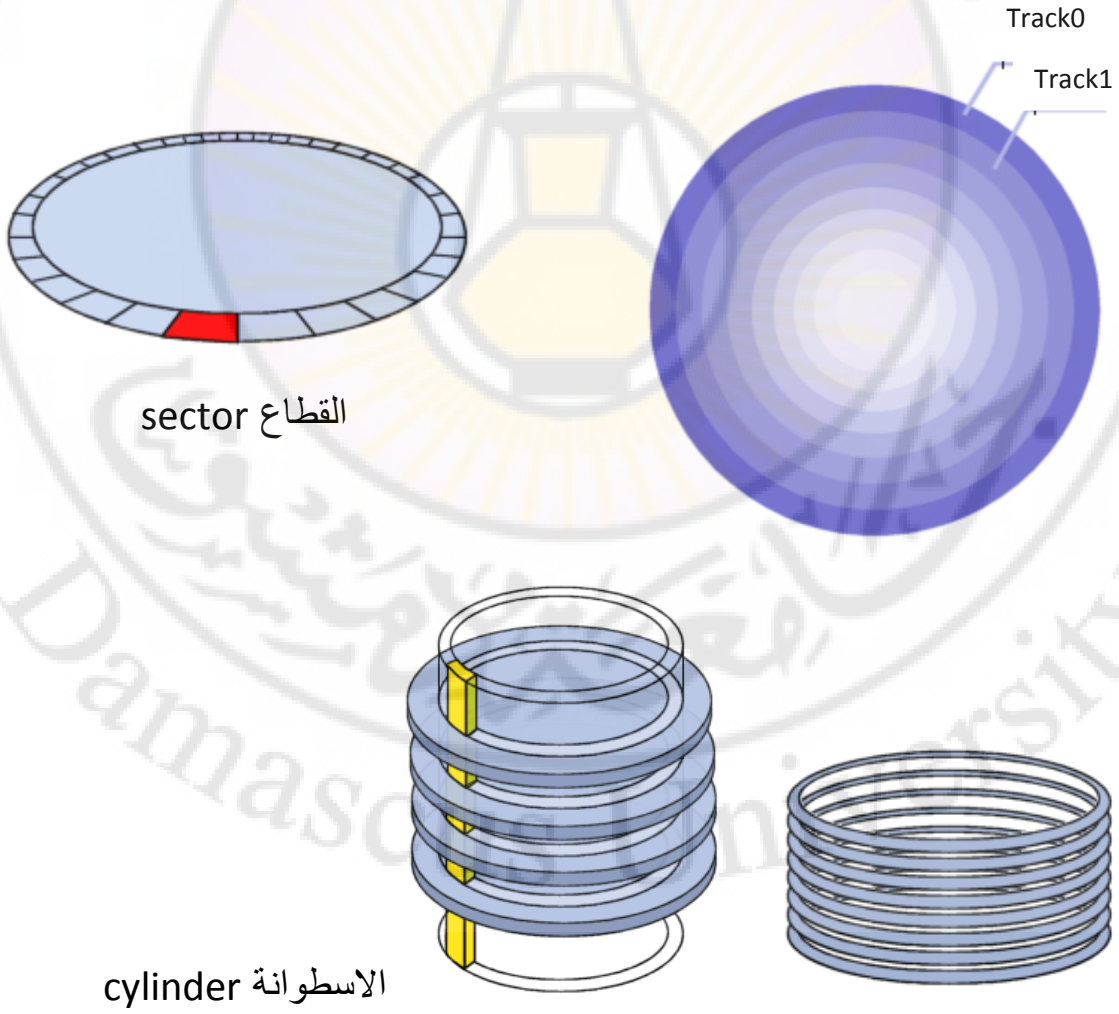
كل قرص بالهارديسك يستخدم رأسين من أجل كتابة وقراءة البيانات رأس قراءة وكتابة من أجل الوجه العلوي من القرص وآخر من أجل الوجه السفلي من القرص. جميع الرؤوس مرتبطة بذراع واحدة لذلك فإنها تتحرك سويا مع بعضها البعض وجميعها تتوضع فيزيائيا على نفس المسار Track. . إذا كان يوجد ثمانية رؤوس ضمن محرك أقراص صلبة معين فسنعلم أنه يحتوي على أربعة أقراص.

4- Actuator Arm(ذراع التحريك): وهي التي تحمل رؤوس القراءة والكتابة و تتمركز على المحرك الذي يدعى Actuator .

أنواع التهيئة للقرص الصلب :

1- التهيئة ذات المستوى المنخفض (Low level format):

تتم هذه العملية في المصنع وتهدف التهيئة المنخفضة إلى تقسيم وجه القرص (أوجه الصفائح) إلى عناصر: مسارات, مقاطع, اسطوانات (cylinders, tracks, sectors), وهي عملية ضرورية لتحضير القرص لإستقبال المعطيات. يجزأ الوجه إلى عدة مسارات يبدأ ترقيمها من 0 ويجزأ المسار إلى مقاطع sectors يبدأ ترقيمها من 1 محددة بشعاعين وبسعة 512 bytes وهي أصغر سعة تخزين بالقرص الصلب . نسمي مجموعة المسارات من أوجه الصفائح والتي تبعد بعداً ثابتاً عن المركز بالإسطوانة cylinder.



2- التهيئة من المستوى المرتفع (high level format)(المنطقية):

وهي المرحلة التي يتم بها تحديد الحجم الخاص لكل جزء من القرص الصلب واعطاءه تسمية مثل C, D, F .. و أي نوع ملفات سوف يستخدمه FAT32 أو NTFS مثلا ويتم نسخ نظام الملفات الخاص على كل جزء ليتم استخدامه فيما بعد.

العوامل CHS:

وهي اختصار ل Cylinder Heads Sectors وهي ثلاث عوامل تحدد هندسة القرص من خلال تحديد عدد الإسطوانات و عدد الرؤوس و عدد القطاعات في كل مسار Track ومن خلال معرفة هذه القيم يمكننا معرفة حجم القرص الكلي وبالعادة تكتب هذه القيم على القرص .

مثلا : لدينا قرص يحوي 4092 اسطوانة (Cylinders) و 16 راس قراءة وكتابة(Heads)و لدينا بكل مسار يوجد 63 قطاع(Sector)فإن حجم القرص الصلب سوف يكون: 4092*16*63 ويساوي

2,111,864,832 بايت والذي يساوي حوالي GB2,1 حيث كما نعلم حجم القطاع هو 512 بايت.

العوامل المؤثرة على أداء الأقراص الصلبة:

1- (سرعة الدوران) Spin speed:

وهو السرعة التي يمكن أن تدور بها الاقراص وتقاس بعدد الدورات بالدقيقة أوRPM اختصار ل Rotation per minute وكلما كانت قيمة هذا المعامل أكبر كلما كان القرص أسرع.

2- (زمن البحث)Seek time:

وهو الزمن اللازم لرأس القراءة والكتابة للوصول للمسارTrack المطلوب.زمن البحث يحسب عادة بشكل وسطي لأن الزمن قد يختلف بحسب تموضع رأس القراءة والكتابة.مثلا : اذا كان رأس القراءة والكتابة بالمسار 1 فإنه سوف يأخذ زمن أطول للإنتقال للمسار 12 من إنتقاله للمسار 3 يقاس زمن البحث بالميللي ثانية.

3- (التأخير)Latency:

وهو الزمن اللازم للقطاع المطلوب Sector حتى يتموضع تحت رأس القراءة والكتابة وذلك بعد إيجاد المسار المطلوب. ويقاس عادة بالميلي ثانية.

4- (زمن النفاذ)Access time:

وهو يمثل الزمن الكلي والممتد من لحظة إعطاء الأمر للقرص الصلب إلى لحظة بدء الحصول على البيانات منه ويمثل مجموع كلا الزمنين زمن البحث + زمن التأخير.

تقنية ATA المتوازية والتسلسلية:

ظهرت عام 1990 واجهة تحكم سميت ATA اختصارا للعبارة Advanced Technology Attachment وقامت بإحتكار كامل سوق محركات الأقراص الصلبة تقريبا وظهر منها عدة معايير **حيث يحدد معيار ATA الأمور التالية :**

1- الطريقة التي يتصل بها الأقراص الصلبة .

2- سرعة نقل البيانات و طريقة نقل البيانات بين متحكم القرص و البيوس و نظام التشغيل على اللوحة الأم.

3- نوع الكبلات و الموصلات المستخدمة لوصل القرص الصلب على اللوحة الأم.

وسوف نتكلم عن كل تعديل بكل معيار من المعايير السبعة بإختصار:

المعيار ATA-1:

- الحجم الأعظمي للقرص بإستخدام هذا المعيار كان بحدود 504 ميغابايت فقط.

- حدد هذا المعيار أنه لايمكن وصل أكثر من محركي أقراص صلبة إلى نفس موصل IDE عبر كبل شريطي واحد.

- استخدم هذا المعيار كبل يدعى Ribbon cable يحوي على 40 سلك ومتحكم IDE واحد على اللوحة الأم.

- وصلت السرعة العظمى لنقل البيانات بهذا المعيار 8.3 ميغابايت في الثانية حيث ظهر مع هذا

المعيار نمطين من نقل البيانات :

1- الدخل والخرج المبرمج PIO(Programmable I/O):

في هذه التقنية يقوم معالج النظام بمعالجة كافة التعليمات اللازمة لنقل البيانات من القرص إلى الرام وبالعكس . لذلك فهي مستخدمة مع محركات الأقراص القديمة فقط. ومع ذلك فقد نجد بعض السواقات الليزرية تستخدم هذه التقنية الآن.

وظهر منها عدة أنماط PIO 0 بسرعة 3.3 ميغابايت في الثانية والنمط PIO 1 بسرعة 5.2 ميغابايت في الثانية و النمط PIO 2 بسرعة 8.3 ميغابايت في الثانية .

2- الوصول المباشر للذاكرة DMA(Direct Memory Access):

لاحاجة لتدخل المعالج في عملية النقل حيث تتم باستخدام قنوات DMA تكون قناة DMA مسؤولة عن عملية نقل البيانات بشكل كامل من القرص الصلب وإلى الذاكرة كما يمكن استخدام DMA مع محركات الأقراص المرنة ومع بطاقات الصوت أيضا.

ظهرت سرعات منها : النمط DMA 0 بسرعة 2.1 ميغابايت في الثانية و النمطDMA 1 بسرعة 4.2 ميغابايت في الثانية والنمط 8.3 ميغابايت في الثانية.

المعيار ATA-2:

- أطلق عليه التسمية EIDE اختصار ل Enhanced IDE حيث سمح هذا المعيار بوصل أربعة أجهزة تخزين وذلك بإضافة متحكم IDE ثاني كل متحكم يوصل إليه كبل يدعى الأول أولي IDE1(Primary) وثانوي IDE2 (Secondary) حيث يوصل على كل كبل جهازي تخزين وعند وصل جهازين على نفس الكبل يتم إعداد احدهما Master والآخر Slave عن طريق ال jumbers في الجزء الخلفي من القرص الصلب. وتدعى الأقراص الموصولة على الكبل الأول Primary master, primary slave والموصولة على الكبل الثاني Secondary master, Secondary slave.

- أضاف المعيار ATA-2 توسيعا أسماه ATAPI اختصار ل ATA Packet Interface الذي جعل من الممكن لأجهزة ليست بمحركات أقراص صلبة (كمحركات الأقراص الليزرية ومحركات الأشرطة المغناطيسية) أن ترتبط بالحاسب عبر متحكم IDE.

- سمح بسرعات أعلى وصلت حتى 16.6 MB/S وذلك بإصدار الأنماط PIO 3, 4 و DMA 1,2

المعيار ATA-3:

بقيت السرعة 16.6 MB/S ولكن أضاف تقنية جديدة اسماها S.M.A.R.T وهي تقنية تساعد بالتنبؤ بالمرحلة التي يبدأ فيها محرك الأقراص الصلبة بالانهيار عن طريقة مراقبة المكونات الميكانيكة له.

ملاحظة : S.M.A.R.T: اختصار ل Self-monitoring, Analysis, and reporting technology

المعيار ATA-4:

وصلت السرعة حتى 33.3 MB/S وذلك باستخدام نمط جديد للنقل اسمه Ultra DMA وظهر منه النمط 0,1,2. وأصبح الكبل المستخدم لوصل الأقراص يحوي على 80 سلك بدل 40 سلك حيث تستخدم 40 سلك لنقل البيانات و 40 سلك يتوضعون بين الأسلاك من أجل إزالة الضجيج الناتج عن المؤثرات الخارجية .

المعيار ATA-5:

وصلت سرعة النقل حتى 66.6 MB/S وذلك بتبني انماط جديدة من Ultra DMA 3,4 ويستخدم كبل 80 سلك أيضا.

المعيار ATA-6:

وصلت سرعة النقل حتى 100 MB/S وعرف نمط 5 من Ultra DMA و كبل 80 سلك ايضا ووصل حجم القرص أكثر من 160 GB.

المعيار ATA-7:

في هذا المعيار ظهرت تقنية SATA أو اختصار Serial ATA ويعتمد النقل التسلسلي بدل النقل المتوازي PATA اختصار ل Parallel ATA الذي ساد من المعيار ATA-2 حتى المعيار ATA-6

ويستخدم في هذا المعيار كبل تسلسلي خاص بال SATA يحوي 7 أسلاك. وسرعة النقل وصلت حتى 300MB/s حيث أصبحت أسرع ب 30 مرة تقريبا من تقنية PATA.

مشاكل ال PATA الذي ساد من المعيارATA-2 حتى المعيار ATA-6:

1- الكبل الخاص بتقنية PATA عريض و يمنع تدفق الهواء داخل صندوق الحاسب.

2- الكبل محدود الطول فقط 45 سم .

3- لاتدعم هذه التقنية خاصية Hot-swap (تبديل القرص بدون اطفاء الحاسب) حيث يجب اطفاء الحاسب عندما نريد استبدال القرص أو تركيب قرص جديد.

4- سرعة نقل البيانات باستخدام هذه التقنية وصلت إلى الحد الأقصى ولايمكن تجاوزها باستخدام النقل التفرعي .

مقارنة بين تقنية SATA و PATA

التقنية	PATA	SATA
نوع النقل	تفرعي (مجموعة بتات سوية)	تسلسلي (بت بت)
عدد الأقراص الممكن وصلها	قرصين على كبل واحد وأربعة أقراص كحد أقصى في الحاسب ككل	لايوجد حد اقصى إنما يعتمد على عدد المنافذ المتاحة على اللوحة الأم.
نوع الكبل وطوله	كبل 40 سلك أو 80 سلك بطول 45 سم	كبل تسلسلي يحوي 7 اسلاك يصل طوله 1 متر.
تقنية Master/slave	يجب تطبيق التقنية عند وصل قرصين على نفس الكبل.	تخلى عن هذه التقنية حيث يتصل كل جهاز مباشرة بالمنفذ نقطة لنقطة .
سرعة النقل	وصلت إلى 133 MB/s كحد أقصى	أسرع ب 30 مرة تقريبا من PATA

كبال ال SATA باللون الأحمر على اليمين و نوعي الكبال الشريطي Ribbon cable: 40 wire و 80 wire

الفيروســـات وأشـــــباهها
Viruses, Worms, Hoax

يمكننا القول إنه لا يوجد أحد لم يسمع بالفيروسات الحاسوبية بل يمكننا أيضاً أن نقول إن القليل من يسلم منها. فعند إجراء مسح لعدد كبير من الشركات لعام 2000م، وجد أن 99،67٪ منهم قد تعرضوا على الأقل لفيروس واحد[1]. ويتراوح عدد الفيروسات الجديدة كل يوم ما بين 10-20 فيروساً جديداً. بل إن شـــــركة F-Secure[2] المتخصصة في مكافحة الفيروسات أضافت 1418 تعريفاً لفيروسات جديدة خلال شهر نوفمبر لعام 2004م. ويقدر عدد الفيروسات المعروفة بقرابة 100000 فيروس. هذا عن تعدادها، فما ذاعن تكلفة أضرارها؟.

تقدر تكلفة ضرر الفيروسات لكل شركة بما يتراوح بين 100000 ومليون دولار أمريكي لكل شركة[3]. وقد قدرت تكلفة أضرار الفيروسات عالمياً لعام 2003م بـ 55 بليون دولار أمريكي وبما يتراوح بين 22-30 بليون دولار أمريكي لعام 2002م، و بـ 13 بليون دولار أمريكي لعام 2001م[4]. لاحظ أننا عندما نتكلم بشكل عام عن الفيروسات، فإننا نعني الفيروسات والديدان (Worms) معاً.

---

(1) Computer Virus Prevalence Survey, 2000.

(2) F-Secure Coropration's Data Secuity Summary for 2005.

(3) Computer Security Institute, 2001.

(4) Mirco Trend Inc.

[1] أنواعها

❖ **الفيروسات Viruses**

هي برامج حاسوبية خبيثة مضرة بالحواسيب، وتنتقل بين الحواسيب بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى. وهناك أنواع للفيروسات، منها ما يبدأ عمله بوقت أو حادثة معينة، حتى أصبح هناك تقويم للفيروسات التي ستعمل في يوم ما[1]، ومنها ما يكون مكوناً من أجزاء متعددة، ومنها ما تتغير صفاته بشكل دوري. ومنها ما يكون متخفياً حتى عن برامج مكافح الفيروسات.

❖ **الديدان Worms**

هي برامج حاسوبية خبيثة ومضرة، وتنتقل بين الحواسيب بعدة طرق، وتمتاز عن الفيروسات باعتماديتها على نفسها لتتكاثر وبسرعة الانتقال وصغر الحجم. والديدان لا تقوم عادة بعمل ضار مباشرة، كحذف البيانات، ولكن سرعة تكاثرها وانتقالها السريعان يؤثران سلباً في فعالية الحاسوب وشبكة المعلومات.

❖ **الخداع أو البلاغ الكاذب Hoax**

البلاغ الكاذب عن ظهور فيروس، يربك به الناس ويضيع به أوقاتهم، وقد يؤثر في الحاسوب. وهو يبدأ من شخص يريد الضرر وينتشر بواسطة أناس صدّقوا الكذبة ونشروا الخبر بغرض المساعدة في التصدي للفيروس أو الدودة. قد تأتيك رسالة بريدية كاذبة تحذرك من فيروس معين قد انتشر مؤخراً، ثم يقدم لك خطوات لمعرفة ما إذا كان جهازك قد أصيب به أم لا. وطبعاً سيكون جهازك مصاباً به لأن الخطوات لاكتشاف الفيروس تدل على أن كل جهاز صحيح مصاب لكي

---

(1) http://us.mcafee.com/virusInfo/default.asp?id=calendar.

يأكل الطعم، ثم يُطلب منك حذف بعض الملفات الأساسية للحماية من الفيروس أو الدودة، وبعد ذلك يتعطل جهازك. هذا مجرد مثال، ولمزيد من أنواع البلاغات الكاذبة يمكنك الرجوع لموقع شركة F-Secure[1].

[2] آثارها

الفيروسات بريمجات خبيثة بطبيعتها؛ فهي تؤثر تأثيراً سلبياً في الحواسيب بشكل مباشر، وفي غير الحواسيب بشكل غير مباشر. فالفيروس عندما يحذف ملفات مهمة للعملاء فإن التأثير يتعدى الحاسوب إلى العملاء وسمعة الشركة. والفيروسات لها تأثيرات شتى، منها: ما يقوم بحذف ملفات أو برامج أو تعطيلها عن العمل، ومنها ما يقوم بزراعة برامج خبيثة أخرى قد تكون تجسسية، ومنها ما يعطل الجهاز بالكلية وغيرها من الآثار الضارة.

وكذلك الديدان لها تأثيرات ضارة. كما هو معروف فإن كل برنامج يعمل في جهازك يأخذ من وقت المعالج، ومساحة في الذاكرة والقرص الصلب، حتى وإن كان البرنامج صغير الحجم، فما بالك إذا كان هناك عدد كبير من البرامج. كذلك عند انتقال ملايين البريمجات الصغيرة عن طريق الشبكة، فإنها تزحم الشبكة وتعطل منافع كثيرة معتمدة على الشبكة، أحد الأمثلة على الديدان المشهورة هو سلامر Slammer، الذي تميز بسرعة انتشار هائلة، ما مكنه من المرور على جميع عناوين الإنترنت IP البالغ عددها 4 بلايين عنوان في غضون 15دقيقة. وأدى انتشار الديدان الواسع إلى إضعاف سرعة النقل على الإنترنت، وأدى إلى تعطيل إحدى أكبر شبكات الصراف الآلي في العالم خلال فترة نهاية الأسبوع، وأبطأ أنظمة التحكم الجوي في كثير من المطارات الدولية. والأدهى من ذلك أنه استطاع أن ينفذ إلى الشبكة الداخلية لمحطة

---

(1) http://f-secure.com/virus-info/hoax/) .

الطاقة النووية في ولاية أهايو في أمريكا، وعَطَّل الحاسوب المسؤول عن مراقبة حالة المفاعل النووي للمحطة. إنه حتى مع صغر حجم هذه الديدان فإنها استطاعت أن تؤثر في حياتنا اليومية. فهذا بلاستر Blaster – نوع من أنواع الديدان– استطاع أن يؤثر في الأنظمة البنكية حول العالم، وأجبر بعض خطوط الطيران والقطارات على إلغاء بعض رحلاتها.

[3] طرق العلاج

يعتمد نوع العلاج على نوع الإصابة وتأثير الفيروس. إذا وصل ضرر الفيروس إلى حذف أغلب الملفات، أو عطّل الجهاز فما لديك سوى إعادة تثبيت جميع البرامج والملفات من النسخة الاحتياطية لملفاتك التي أوصينا بالاحتفاظ بها في طرق الوقاية. أما إذا كان ضرر الفيروس أقل من ذلك فإن برنامج مكافح الفيروسات سيساعدك على إصلاح الملفات المعطوبة قدر الإمكان، وحذف الفيروس من الجهاز. ولا تنس أن تحدّث برنامج مكافح الفيروسات ليتمكن من التعرف على الفيروس إن كان من الفيروسات الجديدة.

[4] برامج علاجية

هناك عديد من برامج مكافحة الفيروسات بأنواع ومميزات مختلفة، منها ما هو مجاني، ومنها ما هو بثمن. وهناك أيضا برامج تعمل على جهازك، ومنها ما يقوم بتفحص ملفاتك وهو على الإنترنت. ومن الأمثلة على تلك البرامج:

أ– البرامج التجارية

McAffe	http://www.mcafee.com
Symantec	http://www.symantec.com
F-SECURE	http://www.f-secure.com
Mirco Trend	http://www.trendmicro.com.

ب– البرامج المجانية

AVG Antivirus	http://free.grisoft.com

جـ – مواقع الفحص عن الفيروسات من على الإنترنت

Mirco Trend	http://housecall.trendmicro.com/housecall/start_corp.asp
RAV Antivirus	http://www.ravantivirus.com/scan/
McAffe	http://us.mcafee.com/root/mfs/
Mirco Trend	http://www.trendmicro.com/

[5] الاستخدام الأمثل لبرامج العلاج

للاستفادة القصوى من برامج مكافحة الفيروسات اتبع الخطوات التالية :

* تأكد دائماً من وجود وعمل برنامج مكافحة الفيروسات على جهازك.

* تأكد من عمل خاصية المراقبة المباشرة – إن وجدت – لكشف الفيروسات حال ولوجها الجهاز.

* تأكد من عمل خاصية مراقبة الرسائل البريدية – إن وجدت- حال تحميلها من جهاز الخادم لكشف وإزالتها الفيروسات قبل تصفح البريد.

* تأكد من تحديث برنامج مكافحة الفيروسات دورياً لكشف الفيروسات الجديدة.

* جدول برنامج المكافحة لتمشيط ملفاتك دورياً وآليا في الأوقات التي لا تعمل بها.

* استخدم جميع الخصائص التي قد تكون في نسخة برنامج المكافحة الذي لديك، مثل: مراقبة برنامج المراسل الآني لكشف تنزيل أي فيروس حال تنزيل ملفات عبر المراسل.

الأحصنة الطروادية
Trojan Horses

يرجع الاسم إلى أسطورة قديمة مفادها أن جيش إحدى مدن الإغريق أهدى أعداءهم حصاناً خشبياً كبيراً، وعندما قبله العدو وجاؤوا به إلى بلدتهم، وفي الليل فتح الحصان فخرج منه جنود استطاعوا السيطرة على البلدة.

وحديثنا هنا عن برنامج حاسوبي يضمر أعمالاً خبيثة ومضرة، خلاف ما يظهره من أعمال مفيدة، وهو لا يتكاثر مثل الفيروسات والديدان، ولكن يكمن في النظام بشكل خفي، يحاول استغلال حاسوبك لشن الهجوم على حواسيب أخرى، أو التجسس من خلال الاحتفاظ بجميع ما أدخلت عن طريق لوحة المفاتيح، والتي قد تحتوي على رقم بطاقة الائتمان، أو كلمة المرور.

[1] أنواعها

الوصول عن بعد: هذه البرامج تسمح للمهاجم بأن يتحكم في جهازك عن بعد بشكل مخفي. من أمثلته : Back Orifice, Netbus.

مرسل البيانات Data Sender: هذا البرنامج يرسل بيانات خاصة بالمستخدم للمهاجم دون علم المستخدم. قد يرسل رقم بطاقات الائتمان، كلمة المرور، محادثاتك المكتوبة وغيرها من البيانات المهمة. يرسل البيانات بواسطة رسالة بريدية، أو تزويدها لموقع المهاجم مباشرة.

معطل الخدمات Denial of service: يعمل هذا البرنامج بالتنسيق مع نُسخ أخرى مشابهة على أجهزة أخرى مهاجمة على مهاجمة حاسوب معين وإغراق شبكته وشلّها.

وسيط Proxy : يُسخر الحاسوب المهاجم وسيطاً يستطيع المهاجم استخدامه

للوصول المتخفّي للإنترنت، بحيث لو عمل عملاً غير شرعي وتمت متابعة العملية فإن الحاسوب الذي جرى تسخيره هو آخر نقطة يمكن تتبع العملية إليها.

معطل البرامج Blocker : يقوم هذا البرنامج، بتعطيل بعض البرامج، خاصة الحساسة، مثل: برامج مكافحة الفيروسات، وبرامج جدران الحماية ليجرد جهازك من أي حماية ضد الهجمات المستقبلية.

[2] طريقة عملها

يقوم المهاجم بزرع برنامج مستقبل أو خادم (Client/ Server) (لاستقبال الأوامر والتعليمات) على جهاز الضحية بعدة طرق ذكرناها سابقاً، ويفتح منفذاً خاصاً به للاتصال عن طريق الإنترنت، ثم يقوم البرنامج بإرسال عنوان جهازك على الإنترنت (IP) للمهاجم، بعد ذلك يقوم المهاجم بالاتصال بذلك البرنامج ليبدأ التحكم بجهاز الضحية.

[3] برامج علاجية

بما أن هناك برنامجاً خبيثاً و منفذاً مفتوحاً للاتصال فإن الحل الأنجع للعلاج من الأحصنة الطروادية يكمن في نوعين من البرامج هما:

* **برنامج جدار الحماية (Firewall)**: للتحكم في المنافذ ومراقبتها، ومنع المنافذ غير الشرعية من الاتصال بالإنترنت، وبالتالي قطع الصلة بالمهاجم. وهذا العمل مهم، لكن لا يفيد في حال اتخذ البرنامج الخبيث قناة أخرى شرعية للاتصال، كأن يستخدم البريد الإلكتروني، أو المراسل الآني. و يمكن للقارئ معرفة المزيد عن برامج جدار الحماية في الجزء الخاص بها في هذا الكتاب.

* **برنامج لصيد البرامج الخبيثة بشكل عام والأحصنة الطروادية بشكل خاص ومكافحتها**: إن برامج مكافحة الفيروسات تصيد جزءاً من الأحصنة الطروادية، لكن ليس

جميعها، لذا يلزمك برامج مكافحة خاصة بالأحصنة الطروادية لحماية جهازك بشكل أفضل، ولا تنس أن تحدّث برامج المكافحة بشكل دوري لصيد البرامج الخبيثة الجديدة.

ومن برامج مكافحة الأحصنة الطروادية:

lockdown2000	http://www.lockdown2000.com
Pest Patrol	http://www.safersite.com
The Cleaner	http://www.moosoft.com
Tuscan	http://agnitum.com/products/tauscan/
Trojan hunter	http://www.trojanhunter.com/
Trojan remover	http://www.simplysup.com/

لا تنس بعد اكتشاف أي حصان طروادي ومكافحته أن تقوم بالتالي:

- استبدل كلمات المرور المسجلة على الجهاز والتي يمكن أن تكون قد سُرقت من قبل المهاجم عن طريق الحصان الطروادي.
- تفحص جهازك باستخدام برنامج مكافحة الفيروسات، تحسباً من أن يكون المهاجم قد زرع فيروساً في جهازك.

رسائل الاصطياد الخادعة

Phishing Scam

كثرت في الآونة الأخيرة طرق الاحتيال والخداع حتى أصبحت أكثر تفنناً وإتقاناً. ومن الطرق المستحدثة ما يسمى رسائل الاصطياد الخادعة، وهي رسائل تبدو بالشكل والعنوان البريدي أنها مرسلة من منظمة حقيقية (وغالباً ما تكون المنظمة بنكاً)، وتفيد بأن هناك تحديثاً للبيانات، أو إجراءات جديدة للحماية والأمن وتطلب منك الدخول لموقع البنك عن طريق الرابط المزود مع الرسالة. وعند الانتقال للموقع الوهمي، الذي يبدو بشكله وتصميمه، وكذلك عنوانه كالبنك المعني، يطلب منك بيانات خاصة، ككلمة المرور، أو معلومات بطاقة الائتمان، ثم بعد الحصول على تلك المعلومات الثمينة يحيلك لموقع البنك الحقيقي.

هناك نمو مطرد يصل إلى 36٪ شهرياً في عدد الرسائل الجديدة من هذا النوع، لقد بلغت وقد بلغ عدد رسائل الاصطياد الخادعة 6597 رسالة مختلفة في شهر أكتوبر لعام 2004م.

لنأخذ مثالاً واقعياً على هذه الطريقة سجلته مجموعة مكافحة رسائل الاصطياد[1].

لنفرض أنك أحد عملاء بنك يدعى SunTrust Bank ؛ وجاءتك رسالة نصها:

---

(1) http://www.antiphishing.org/.

Dear SunTrust Bank Customer,

To provide our customers the most effective and secure online access to their accounts, we are continually upgrading our online services. As we add new features and enhancements to our service, there are certain browser versions, which will not support these system upgrades. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

In order to further protect your account, we have introduced some new important security standards and browser requirements. SunTrust security systems require that you test your browser now to see if it meets the requirements for SunTrust Internet Banking.

Please sign on to Internet Banking in order to verify security update installation. This security update will be effective immediately. In the meantime, some of the Internet Banking services may not be available.

SunTrust Internet Banking

الشكل رقم (10): رسالة اصطياد

فحوى الرسالة أن البنك قام بتعزيز أنظمة الحماية وتحديث خدماته البنكية الشبكية، ويريد منك التأكد من أن برنامج متصفح الإنترنت الذي تعمل عليه متوافق مع التحديثات الجديدة، لذا يلزمك الدخول لموقع البنك والتسجيل بواسطة الضغط على الرابط المعطى. وعند الضغط على الرابط يحولك إلى موقع البنك المزيف كما هو موضح بالشكل (11).

الشكل رقم (11): موقع البنك المزيف.

الموقع يبدو حقيقياً لسببين قد يصدقهما المستخدم:

أولاً: التصميم قريب جداً للموقع الحقيقي.

ثانياً: العنوان (URL) يبدو حقيقياً وهو:

(http://internetbanking.suntrust.com).

لقد تحايلوا بتغطية شريط العنوان بشريط آخر معمول بلغة جافا. ويمكن معرفته بالضغط بالزر الأيمن للفأرة على شريط الأدوات، ثم اختيار خصائص، ثم تمريره على شريط العنوان ليتضح أن شريط العنوان مغطى كما هو موضح في الشكل. شريط العنوان الحقيقي يشير إلى الموقع المزيف بعنوان: (http://82.90.165.65/s/login.html). طبعاً بعد أخذ معلوماتك السرية يخبرك بأن برنامج المتصفح متوافق مع الخدمات الجديدة، ثم يحيلك إلى موقع البنك الحقيقي، وكأن شيئاً لم يكن، حتى لا يثير شكك! وإذا كنت من عملاء البنك وتستخدم الخدمات النسيجية للبنك وجاءتك مثل تلك الرسالة فإنك قد تصدّقهم، خاصة أنه طلب منك المعلومات عن طريق موقعهم، والذي يبدو حقيقياً.

[1] طرق الوقاية

* كن حذراً من الرسائل التي تطلب بشكل مستعجل معلومات شخصية سرية.

* رسائل الخداع موجهة للعموم؛ أما الرسائل المرسلة من الجهات الحقيقية فتكون مخصوصة باسمك.

* لا تستخدم الرابط، بل قم بمحادثة الجهة مباشرة، أو اكتب بنفسك موقع الجهة في شريط العنوان على برنامج متصفح الإنترنت مباشرة.

* لا تقم بتعبئة أي نموذج بالبريد الإلكتروني. تعبئة بياناتك لابد أن تكون عن

طريق موقع ومحمي بالتأكد من أن العنوان يبدأ بـ https وليس http فقط ، وشكل القفل التالي 

في زاوية المتصفح السفلى.

* حدّث برنامج المتصفح و نظام التشغيل بأحدث الترقيات الأمنية.

لكن إذا أكلت الطعم وقدّمت بيانات سريه فعليك الإبلاغ في أسرع وقت ممكن للجهة الحقيقة لإلغاء البطاقة واستبدال بطاقة ورقم جديدين بها ، أو تغيير رقم الحساب ، أو كلمة المرور ، أو اسم المستخدم ، أو غيرها من الإجراءات اللازمة لتلافي أي خسائر.

لا تعد المراسلات الإلكترونية وثائق رسمية لدى المؤسسات المالية مثل البنوك ، لذا ينصح الحذر من الرسائل الإلكترونية المرسلة من قبل البنوك و التي تطلب معلومات سرية ، فقد تكون تلك الرسائل غير صحيحة المصدر.

البرامج التجسسية و أشباهها
Spyware

البرامج التجسسية هي كل برنامج يراقب سلوكك على جهازك من مراقبة كتاباتك إلى مراقبة المواقع التي تزورها. والهدف من برامج التجسس يكاد ينحصر في أمرين: أولهما: التجسس الخبيث لاستسقاء معلومات سرية، مثل كلمات المرور، وأرقام الحسابات البنكية، و والآخر: لأغراض تجارية، مثل: معرفة أنماط المستخدم الاستهلاكية، أو محركات البحث الأكثر استخداماً، أو المواقع التجارية الأكثر تسوقاً.

إن تلك البرامج تستنزف طاقات الجهاز والاتصال دون إذن واضح منك. وكما تعلم أن مجرد المراقبة، وتسجيل السلوك أو المعلومات يتطلب وقتاً من المعالج، ومساحة من الذاكرة، ووحدة التخزين الدائمة، وجزءاً من كمية البيانات المرسلة عن طريق وسيط الاتصال.

[1] أنواعها

* **برنامج متابعة تصرفات المستخدم أو التجسس البسيط Spyware**

هي كل برنامج يتجسس على سلوك المستخدم أو معلوماته بعلم، أو بدون علم.

* **برنامج تسجيل نقرات لوحة المفاتيح Keystroke Logger**

تخيل أن كل ما تكتبه على لوحة المفاتيح يُسّجل وقد يُرسل لغيرك. نعم كل شيء، من رسائل بريدية إلكترونية، ودردشة، إلى كلمات المرور، وأرقام بطاقاتك البنكية. هناك برامج وقطع إلكترونية لعمل ذلك، وهي تُسَوق على أنها برامج مراقبة لأب على أبنائه أو لزوج على زوجته، أو العكس. لكن في الوقت نفسه تُستخدم تلك البرامج استخداماً خبيثاً، كأن تُزرع تلك البرامج في جهازك – من غير علمك – بواسطة أحد مهاجمي

جهازك، ويتلقى ما تكتبه بشكل مستمر. وبرنامج تسجيل نقرات لوحة المفاتيح هو نوع من أنواع برامج التجسس Spyware، والأحصنة الطروادية.

*** برامج الإعلانات Adware**

هي برامج أو بريمجات هدفها التسويق التجاري بطريقة إجبارية غير مرغوبة. ومن الأمثلة على تلك البرامج:

(1) تقديم إعلانات لمنتجات معيّنة بمجرد البحث، عن مثيلاتها في محرك البحث.

(2) تعطيل محرك البحث وتقديم محرك بحث آخر مقلد ليخدم مهام الجهة الإعلامية لبرنامج الإعلانات.

(3) تحويل المستخدم إلى مواقع تجارية دون إذنه.

*** الصفحات الفقّاعية أو الانبثاقية Popup**

هي برامج فقّاعية أو انبثاقية تخرج بين الفينة والأخرى، كإعلانات أثناء تصفح الإنترنت، وتستهلك موارد النظام والاتصال، خاصة إذا كان الاتصال بسرعة 56 كيلوبت/ثانية. وقد تؤدي البرامج الفقاعية إلى مشاكل أمنية جرّاء الإخفاق في سد الثغرات الأمنية للحاسوب.

[2] طرق الإصابة بها

تتمكن تلك البرامج من النزول في حاسوبك باستخدام إحدى طريقتين:

أولاهما: عن طريق وجودها مع البرامج المجانية أو المشبوهة.

والأخرى: عن طريق استغلال إحدى الثغرات الأمنية في جهازك للوصول إليه.

[3] طرق معرفة الإصابة بها

هناك عدة طرق للتعرف على الإصابة ببرامج التجسس والمراقبة، من أوضحها:

* كثرة الصفحات الانبثاقية التي ليس لها صلة بالموقع المزار، مثل صفحات بصور إباحية.

* حاسوبك يحاول الاتصال بالهاتف دون أمرك. وهناك برامج تقوم بالاتصال عن طريق هاتفك ودون أمرك وعلمك بأرقام هواتف دولية باهظة التكلفة.

* يصبح حاسوبك بطيء الاستجابة لدرجة ملحوظة.

* عندما تقوم بالبحث فإن المتصفح يستخدم محركاً للبحث غير الذي حددته.

* قائمة المواقع المفضلة في برنامج متصفح الإنترنت يحتوي على مواقع لم تقم بإضافتها.

* صفحة البداية تشير إلى موقع لم تقم باختياره كصفحة بداية، ويبقى كذلك حتى لو غيرت صفحة البداية.

[4] طرق الوقاية

هناك عدة طرق وقائية ضد برامج التجسس وغيرها من البرامج الضارة:

* داوم على سد الثغرات الأمنية بمتابعة آخر التحديثات لبرامجك الحساسة مثل: نظام التشغيل، ومتصفح الإنترنت، وبرنامج البريد الإلكتروني.

* دعّم حاسوبك ببرنامج أو جهاز جدار الحماية لتقليل تعرّضه للاختراق من قبل الغير.

* دعّم حاسوبك ببرنامج مكافح الفيروسات.

* عند الحاجة لبرامج مجانية حمّلها من مواقع معروفة مثل www.download.com.

* اقرأ محتويات الاتفاقية الخاصة باستخدام البرامج، لأن بعضها تنص بوضوح على أن البرنامج سيقوم بمراقبة سلوكك وإرسال بيانات لجهة خارجية.

* تحاش زيارة المواقع المشبوهة مثل المواقع الإباحية، و مواقع القرصنة.

* تحاش برامج المشاركة P2P.

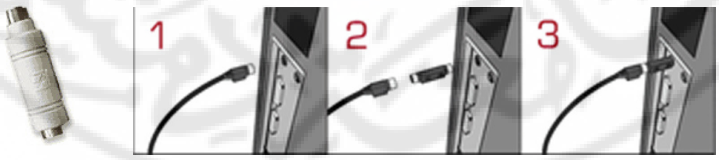
* تأكد من مرفقات رسائل البريد الإلكتروني، ولا تقم بفتحها حتى تتأكد من خلوها من الفيروسات، وأنها مرسلة من شخص موثوق به ومعروف، ومتوقعة الوصول.

* تفحص حاسوبك بشكل دوري باستخدام برنامج مكافحة الفيروسات، وبرنامج مكافحة برامج التجسس.

* دعّم حاسوبك ببرنامج لمكافحة برامج التجسس، والصفحات الفقاعية. وإذا كان حاسوبك مزوداً بالتحديث الجديد لنظام الويندوز اكس بي SP2 فيمكنك استخدام خاصية إيقاف الرسائل الفقاعية، ويمكن تفعيلها من برنامج متصفح الإنترنت تحت قائمة "أدوات"، كما في الشكل رقم (12).

الشكل رقم (12): خاصية إيقاف الرسائل الفقاعية

* تأكد من أن نهاية سلك لوحة المفاتيح موصول بشكل مباشر للحاسوب ولا توجد قطعة بينهما.



الشكل رقم (13): وصل لوحة المفاتيح بالحاسوب.

* تأكد من أن مستوى الأمان في برنامج متصفح الإنترنت مرتفع كما في الشكل

التالي رقم (14).

الشكل رقم (14): مستوى الأمان في برنامج متصفح الإنترنت.

[5] برامج علاجية

هناك برامج عديدة لمكافحة برامج التجسس، منها على سبيل المثال:

Ad-Aware Pro.	http://www.lavasoft.de
Destroy & **Search - Spybot**	http://www.safer-networking.org/en/index.html
Pest Patrol	http://www.pestpatrol.com/

الخلاصة

البرامج الخبيثة هي برامج يكون كل مهامها أو أحدهما عمل إفسادي،

كالتجسس أو التخريب، أو استنزاف الموارد الحاسوبية. و تنتقل هذه البرامج إلى الحاسوب، أو شبكة المعلومات بوسائل متعددة و ملتوية ترتكز في معظمها على استدراج المستخدم. وينبغي أن يتفطن المستخدم لهذه الطرق؛ كما ينبغي أن يتبع الأساليب التي ثبت نجاحها لمنع الإصابة بالبرامج الخبيثة ابتداء، أو التعامل الصحيح معها في حال وصولها إلى شبكة المعلومات.

جدران الحماية
Firewall

إن الفوائد والخدمات التي جاءت بها شبكة الإنترنت لم تأت خلواً من المنغصات، فراجت سوق الطفيليين (Hackers) الذين لا هم لهم سوى التلصص على معلومات الآخرين. كما ظهر أناس يستمتعون بإلحاق الأذى بالآخرين، إما بحذف وثائقهم المهمة، أو العبث بمحتوياتها، أو نشر البرامج السيئة (Malware) مثل الديدان، والفيروسات، وأحصنة طروادة وغيرها.

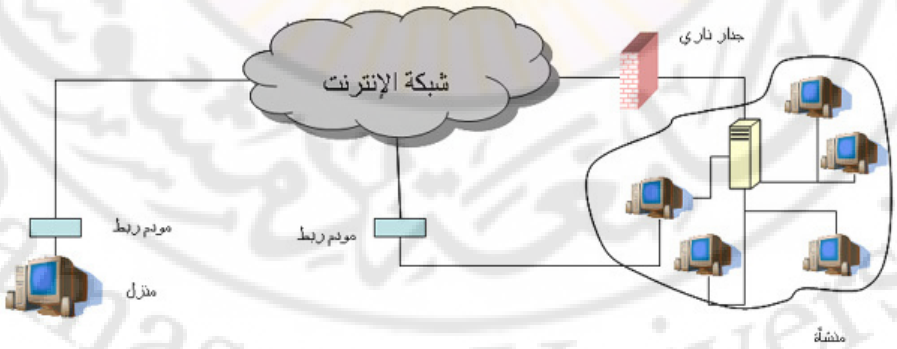
ولمقاومة تلك الأخطار والحد منها ظهرت تقنيات ومفاهيم متعددة، من أكثرها انتشاراً جدران الحماية (Firewalls) التي تسمى أيضا الجدران النارية. ولتقريب المعنى للأذهان نقول إن جدار الحماية نظام مؤلف من برنامج (software) يجري في حاسوب، وهذا الحاسوب قد يكون حاسوبا عاديا، مثل الحاسوبات الشخصية، أو حاسوبا بني بمواصفات خاصة ليكون أكثر قدرة على تلبية المتطلبات الفنية الخاصة بجدار الحماية. وفكرة جدار الحماية تشبه فكرة نقطة التفتيش التي تسمح بمرور أناس، وتمنع مرور آخرين، بناء على تعليمات مسبقة.

[1] وضع جدار الحماية

ولتوفير بعض الحماية لنفسها تقوم المنشآت بوضع جدار حماية لعزل شبكتها الداخلية عن شبكة الإنترنت، كما يوضح الشكل (15). بيد أن هذا العزل لا يمكن أن يكون كلياً؛ وذلك للسماح للجمهور بالاستفادة من الخدمات المقدمة، وفي الوقت ذاته منع الطفيليين والمخربين من الدخول، وتتاح من خلال البرنامج الموجود في جدار

الشكل رقم (15) : وضع جدار الحماية.

الحماية مراقبة المعلومات بين الشبكة الداخلية للمنشأة والعالم الخارجي. ولتحقق الغاية من جدار الحماية فإنه لا بد من وضعه في موقع استراتيجي يضمن ألا تخرج المعلومات أو تدخل إلى الشبكة الداخلية إلا عن طريقه. ولذلك فإن الوضع الموضح في الشكل رقم **(16)**غير مقبول عند المختصين في مجال أمن المعلومات ؛ لأن الوصول للشبكة الداخلية ممكن عن طريق الاتصال بجهاز المودم الذي يشكل في هذه الحالة بوابة خلفية يلج المتطفلون والمخربون عبرها.



الشكل رقم (16): وضع غير محبذ لاستخدام جدار الحماية

[2] كيف تعمل جدران الحماية؟

طريقة عمل جدران الحماية يحددها تصميم جدران الحماية. لتبسيط هذا الموضوع نقول إن هناك ثلاثة أساليب في تصميم جدار الحماية هي :

(أ) أسلوب غربلة مظاريف البيانات المرسلة (Packet Filtering)

تنتقل المعلومات على شبكة الإنترنت في صورة مظروف إلكتروني. وإذا كان جدار الحماية مصمما بهذه الطريقة فإنه يفحص كل مظروف يمر عبره، ويتحقق من تلبية المظروف لشروط معينة يحددها الشخص الذي يدير جدار الحماية، وهذه الشروط تدخل بطريقة خاصة في البرنامج المكون للجدار الناري.

(ب) أسلوب غربلة المظاريف مع تغيير عناوين المظاريف القادمة من الشبكة الداخلية (أي المظاريف الصادرة)

عندما يقوم مستخدم حاسوب ما بالتعامل مع شبكة الإنترنت، مثل أن يتصفح موقعا ما، أو يرسل بريداً إلكترونياً فإن هناك أمورا كثيرة تدور خلف الكواليس دون أن يشعر بها المستخدم. ومن ذلك أن نظام التشغيل الموجود في الحاسوب يقوم بإرسال بيانات إلى شبكة الإنترنت لتحقيق رغبة المستخدم، سواء كانت تصفح موقع، أو إرسال بريد. وهذه البيانات يجمعها الجهاز في مظاريف إلكترونية تحمل –ضمن ما تحمل من معلومات– العنوان الرقمي المميز للحاسوب الذي أرسلها، أو ما يسمى (IP Address). وهذا العنوان يميز هذا الجهاز عن سائر الأجهزة المرتبطة في شبكة الإنترنت، كما سنوضح في موضع آخر من الكتاب. وفائدة هذا العنوان هي تمكين الأطراف الأخرى من إرسال الردود المناسبة للحاسوب الذي أرسل البيانات، وبالتالي تقديم الخدمة للمستخدم الذي طلبها. لكن هذا العنوان قد يُستخدم من قبل أصحاب المآرب السيئة لشن هجمات على ذلك الحاسوب.

وعند اعتماد أسلوب غربلة المظاريف مع تغيير عناوين المظاريف الصادرة يقوم

جدار الحماية بطمس العنوان المميز للحاسوب الذي أرسل المظروف من المظروف الإلكتروني، ووضع العنوان الخاص بالجدار نفسه بدلا منه. وبهذا لا يرى الأشرار المترصدون من الشبكة الداخلية سوى جدار الحماية، فيحجب الجدار كل أجهزة الشبكة المراد حمايتها، وينصب نفسه وكيلاً (Proxy) عنها. وعندما يرغب الموقع المتصَفح الرد فإنه يرسل رده في مظاريف تحمل عنوان جدار الحماية، وبهذا تأخذ كل المظاريف القادمة (الواردة) إلى الشبكة الداخلية عنوان جدار الحماية، ويقوم هو عند استلامها بغربلتها، ثم توجيهها إلى وجهتها النهائية. ولابد في هذه الحالة أن يحتفظ الجدار بجدول متابعة يربط فيه بين عناوين المظاريف الصادرة والواردة. وهذا التنظيم يوفر مقداراً أكبر من الحماية مقارنة بالطريقة الأولى؛ لأن الجدار يحجب عناوين الشبكة الداخلية، مما يصعب مهمة من أراد مهاجمتها. وهذه التقنية تعرف باسم تحويل العناوين الرقمية (Network Address Translation)، أو (NAT) اختصارا، و سنتناولها بشيء من التفصيل في موضع آخر.

(جـ) أسلوب مراقبـــــة السياق (Stateful Inspection)

هنا يقوم جدار الحماية بمراقبة حقول معينة في المظروف الإلكتروني، ويقارنها بالحقول المناظرة لها في المظاريف الأخرى التي في السياق نفسه، ونعني بالسياق هنا مجموعة المظاريف الإلكترونية المتبادلة عبر شبكة الإنترنت بين جهازين لتنفيذ عملية ما. وتجري غربلة المظاريف التي تنتمي لسياق معين إذا لم تلتزم بقواعده؛ لأن هذا دليل على أنها زرعت في السياق وليست جزءاً منه، مما يولد غلبة ظن بأنها برامج مسيئة، أو مظاريف أرسلها شخص متطفل .

وهناك عدة معايير يمكن استخدام واحد منها أو أكثر لتمييز صحيح المظاريف

من سقيمها، ومن هذه المعايير ما يلي:

أ- العنـــــوان الرقمـــــي (IP Address): وهـــو - كما أشرنا سابقا - رقم يميز كل جهاز مشترك في شبكة الإنترنت، فيمكن للجدار الناري أن يجيز مرور مظروف ما، أو يمنعه بناء على العنوان الرقمي للمرسل أو المستقبل.

ب- اسم النطاق (Domain Name) : ليسهل على المستخدم العادي الوصول إلى المواقع على شبكة الإنترنت فإن المواقع تعطى أسماء ذات معنى، إضافة إلى العناوين الرقمية المذكورة سابقاً. فمثلاً اسم النطاق (www.ksu.edu.sa) يدل على موقع جامعة الملك سعود على شبكة الإنترنت، بينما يدل (www.moe.gov.sa) على موقع وزارة التربية والتعليم في المملكة العربية السعودية. وتمكن برمجة جدار الحماية بحيث يمنع مرور المظاريف الإلكترونية القادمة من نطاق (Domain) معين.

(جـ) بروتوكول التخاطب المستخدم: المقصود بالبروتوكول هنا الطريقة المعينة للتخاطب وتبادل المعلومات بين طالب الخدمة والجهة التي تقدم تلك الخدمة. وطالب الخدمة هنا قد يكون إنساناً، أو برنامجاً مثل المتصفح (Browser). وبسبب تنوع الخدمات التي تقدم في شبكة الإنترنت، فإن الشبكة تعج بالبروتوكولات اللازمة لتسهيل تقديم تلك الخدمات لمن يريدها، ومن هذه البرتوكولات:

(1) بروتوكـــول (HTTP): يستخدم لتبادل المعلومات بين برنامج المتصفح ومزود الخدمة في الموقع الذي يزوره المتصفح.

(2) بروتوكول (FTP): يستخدم لنقل الملفات خاصة كبيرة الحجم منها، بدلاً من إرسالها كمرفقات (Attachments) في البريد الإلكتروني .

(3) بروتوكول (SMTP): يستخدم لنقل البريد الإلكتروني.

(4) بروتوكول (SNMP): يستخدم لإدارة الشبكات، وجمع المعلومات عن بعد.

(**5**) **بروتوكول (Telnet)**: يستخدم للدخول على جهاز ما من بعد، وتنفيذ بعض الأوامر داخله.

وهنا نقول إن الشخص المسؤول عن جدار الحماية يمكنه برمجة جدار الحماية بحيث يغربل المظاريف بناء على البروتوكول المستخدم لتراسل البيانات، وهناك خانة في المظروف تدل على نوع البروتوكول، فيقوم جدار الحماية بمعاينتها، فإن وجد أن البروتوكول مسموح به فإن جدار الحماية يسمح للمظروف بالمرور، وإلا فإنه يحذف المظروف.

وهناك معايير أخرى يمكن استخدامها أساساً للغربلة، مثل رقم المنفذ الذي سيستقبل المظروف في الجهاز المرسل إليه. كما يمكن برمجة بعض جدران الحماية للبحث عن كلمات أو عبارات معينة في المظاريف، فتحذف منها ما يحتوي على تلك العبارات وتمرر الباقي.

[3] أنواع جدران الحماية

يمكن تصنيف جدران الحماية من حيث الجهة المستفيدة منها إلى ما يلي:

(أ) **جدران نارية لحماية المنشآت الكبيرة (Enterprise)**: وهذا النوع توفره شركات كبرى متخصصة مثل (CISCO) و(Nortel) و(Symantec). وغالباً ما توفر الشركة المصنعة أنواعاً متعددة من جدران الحماية تتفاوت من حيث سرعتها والخدمات التي تقدمها. وهذا النوع من جدران الحماية يتميز بما يلي:

(1) إن جدار الحماية يكون –غالبا– في جهاز قائم بذاته مصمم لغرض معالجة البيانات بسرعة فائقة، أي أنه ليس مجرد برنامج يعمل في جهاز حاسوب عادي.

(2) تعدد الخدمات التي يقدمها جدار الحماية، مثل: غربلة المظاريف، والحماية ضد الفيروسات، وحماية البريد الإلكتروني، والتشفير.

(3) تشغيل جدار الحماية يحتاج إلى مهارات فنية متقدمة.

(4) ارتفاع كلفة الشراء والتشغيل.

والشكل (17) يظهر صورة لأحد جدران الحماية التي تصنعها شركة (CISCO).

الشكل رقم (17): جدار حماية من شركة CISCO.

(ب) جدران نارية لحماية المنشآت الصغيرة: و هذا النوع يشبه سابقه في كونه جهازا مخصصا قائما بذاته، إلا أنه لا يجاريه من حيث سرعة معالجة البيانات، أو تعدد الخدمات المقدمة، ولهذا فإنه أقل سعراً. من سابقه.

(جـ) جدران نارية لحماية الأجهزة الشخصية: جدران الحماية هذه في أغلبها ما هي إلا برامج تحمل في الحاسوب الشخصي، بحيث تمر من خلالها جميع المعلومات الخارجة من الحاسوب أو الداخلة إليه. وفي هذا المجال أيضا يتنافس عدد من الشركات على السوق الكبير لجدران الحماية الشخصية. ومن أمثلة المنتجات في هذا المجال ما يلي:

(1) Norton Personal Firewall
(2) ZoneAlarm .
(3) Sygate
(4) McAfee

و يقدم هذا النوع من جدران الحماية عدة خدمات، مثل غربلة المظاريف، والحماية ضد الفيروسات، وحماية البريد الإلكتروني، والتشفير، والوقاية من برامج التجسس (Spyware). و يمكن تنزيل هذه البرامج من شبكة الإنترنت، إما مجاناً مثل: (ZoneAlarm)، أو بثمن مثل (ZoneAlarm Pro).

وفي الشكل (18) توضيح للشاشة الرئيسة للجدار الناري ZoneAlarm مع وصف لأهم وظائفه.

و عندما يحاول برنامج موجود داخل الحاسوب الاتصال بالخارج، كالاتصال بموقع موجود على شبكة الإنترنت، يقوم جدار الحماية (ZoneAlarm) بعرض رسالة كتلك الموضحة في الشكل رقم (19)، ويطلب من المستخدم اتخاذ القرار بشأن السماح للبرنامج بالاتصال بالخارج، أو منعه من ذلك. وبهذه الآلية يمنع جدار الحماية البرامج الخبيثة التي قد توجد في جهاز المستخدم من تسريب المعلومات المخزنة في الجهاز إلى الخارج دون علم المستخدم.

الشكل رقم (18): الشاشة الرئيسة لجدار حماية من ZoneAlarm .

الشكل رقم (19): رسالة تحذيرية من جدار الحماية.

كما أن جدار الحماية يمكن تهيئته بحيث يعرض رسالة تحذيرية في كل مرة يحاول برنامج موجود بالخارج الاتصال بالحاسوب الذي يوجد به جدار الحماية، والغرض من هذا واضح، فإنه توجد في شبكة الإنترنت برامج خبيثة كثيرة تحاول الوصول إلى الحواسيب لإتلافها، أو إتلاف البيانات التي فيها.

الخلاصة

بسبب كثرة الأخطار التي تهدد شبكات المعلومات من خارجها، نشأت فكرة إقامة جدران الحماية التي تسمى أيضا الجدران النارية، التي يمكن وصفها بأنها نظام مؤلف من برنامج (software) يعمل في حاسوب، وهذا الحاسوب قد يكون حاسوبا عاديا مثل الحاسوبات الشخصية، أو حاسوبا بني بمواصفات خاصة ليكون أكثر قدرة على تلبية المتطلبات الفنية الخاصة بجدار الحماية. وفكرة جدار الحماية تشبه فكرة نقطة التفتيش التي تسمح بمرور أناس، وتمنع مرور آخرين، بناء على تعليمات مسبقة. وتتعدد أنواع جدران الحماية بحسب حجم منظومة المعلومات المراد حمايتها والتقنية المستخدمة، و يجب تاكيد أهمية وجود جدران الحماية الشخصية بوصفها أحد خطوط الدفاع الأخيرة.

الجيل الأول

Processor Name

Intel® Core™ i7-940 processor

Brand Number

لا يوجد رقم يميزه، حيث يكون موديل المعالج 3أرقام فقط وليس . 4

الجيل الثاني :

Processor Name

Intel® Core™ i7-2600 processor

Brand Number

يطلق عليه Sandy bridge ويميز بالرقم ٢

الجيل الثالث:

يطلق عليه Ivy bridge ويميز بالرقم ٣

الجيل الرابع :

يطلق عليه Haswell ويميز بالرقم ٤

الجيل الخامس :

يطلق عليه Broadwell ويميز بالرقم ٥

الجيل السادس :

يطلق عليه SKYLAKE ويميز بالرقم ٦

الجيل السابع :

يطلق Kaby Lake ويميز بالرقم ٧

اللواحق Suffixes

قد ذكرنا أن اللواحق هي حرف أو أكثر يوجد آخر اسم المعالج ويدل على بعض خصائصه، تنقسم اللواحق إلى لواحق خاصة بالابتوبات وأخرى للحواسيب المكتبية.

لواحق الحواسيب المكتبية:

بلا لاحقة(No suffix)

عندما لا يوجد في اسم المعالج لاحقة يكون هذا المعالج خالي من أي خصائص مميزة، أي أن هذا النوع من المعالجات هو معالج خام أي المعالج الأصل قبل التعديل عليه وإضافة المميزات التي توفرها اللواحق.

T

عندما توجد هذه اللاحقة في اسم معالج ما فهي تعني أداء أقل مع استهلاك طاقة أقل. وهو مشابه للاحقة S ولكن أقل منها، فيكون ترشيد استهلاك الطاقة في T أكبر من S وبذلك معالجات S أقوى من T بقليل.

لا انصح بهذه الفئة من المعالجات للألعاب .

X

تمثل معالجات فائقة القوة و تكون تلك المعالجات قابلة لكسر السرعة حيث تكون ((unlocked

K

تدل على أن المعالج ((unlocked بمعنى قابلية المعالج لكسر السرعة . وهو مشابه للاحقة X

E

هي اختصار ((Embedded وتعني أن هذا المعالج يأتي مدمج مع اللوحة الأم .

P

قديما كان يدل على أن المعالج لا يحتوي على معالج رسومي (كارت شاشة) مدمج به، أما الآن يدل على احتواء المعالج على كارت شاشة ولكنه ضعيف.

C

تدل على معالج ((Unlocked مدمج معه كارت شاشة قوي، والمقبس الخاص به هو H3المعروف((LGA1150

لواحق الحواسيب المحمولة:

U

هي اختصار Ultra-low power وهي اللاحقة الأكثر انتشارًا في الحواسيب المحمولة الآن، يميز هذه المعالجات توفيرها لطاقة البطارية لتستمر معك لأطول وقت ممكن و يسيئها احتوائها على نواتين فقط.

H

يحتوي على نواتين ويستهلك طاقة قليلة ولكنه يحتوي على معالج رسوميات قوي إلى حد ما.

HQ

يشابه اللاحقة H ولكنه يحتوي على ٤ أنوية بدلا من ٢ .

HK

مثله مثل H ولكن يكون ((Unlockedأي يقبل كسر سرعته.

M

وهي اختصار Mobile وتعني أنها مصممة لـ Ultrabooksأو Notepadsأو Laptop وإذا كانت اللاحقة بهذا الشكل "MQ" تعني احتواء المعالج على ٤ أنوية

أعلنت شركة Intel منذ أيام عن إصدار الجيل الثامن من معالجاتها بمعماريتي Coffe Lake) و Cannon Lake)، ولربما نشهد تطورًا كبيرًا في الأداء بدرجة تصل إلى ٤٠ % عن المعمارية السابقة من الجيل السابع والمسماة بـKaby Lake

ولكن مهلًا ... جيل ثامن؟ متى بدأ الجيل الأول؟ هل هو جيل Pentium و Celeron والمعالجات التي كنا نستخدمها في أجهزتنا القديمة وقتما كانت أقوى الألعاب على الساحة هي Virtua Cop و Fifa98؟ أم يُقصد بها معالجات أقدم من تلك المرحلة؟ وما هو الفارق الحقيقي أصلًا بين جيل وآخر؟ وما هو معنى Kaby Lake و Coffe Lake و ... Cannon Lake إلخ؟

المعالج Processor/Central Processing Unit (CPU)

المعالج هو مجرد قطعة صغيرة في جهازك لا تحتل مساحة كبيرة كالتي تحتلها اللوحة الأم أو كارت الشاشة أو أي مكون آخر، ولكنها القطعة الأهم والأكثر تعقيدًا في تصنيعها وفي عملها وفي أهميتها، فهي تمثل فعليًا عقل الكمبيوتر!

المعالج مسؤول عن التعامل مع المليارات من التعليمات في الثانية (نعم المليارات في الثانية الواحدة)، حيث يقوم بتنفيذ التعليمات التي تعطيها له بشكل مباشر أو التي قد لا تشعر بها أساسًا، ولكنها ضرورية لكي تستمر الأمور بشكل طبيعي.

عندما يرغب الكثير من المستخدمين في شراء معالج ما فإنّ الأسئلة الشائعة لا تخرج عن نطاق سرعة المعالج وعدد الأنوية Cores الموجودة به، ولكن هل هذا حقًا هو كل ما يهم؟ لنرى.

سرعة المعالج Clock Speed

تعتبر سرعة المعالج هي الخاصية الأشهر، كانت تقاس قديمًا بالميجاهرتز MHz أمّا الآن فهي تقاس بالجيجا هرتز GHz وهو فارق جنوني في السرعة (ألف ضعف)، على سبيل المثال فإنّ معالج بسرعة ٣ GHz يمكنه القيام بعدد من التعليمات يقدر بثلاثة مليار في الثانية الواحدة.

يمكننا القول أنّ تنفيذ أي مهمة هو بالأساس تنفيذ لعدد معين من التعليمات التي يجب أن يتعامل معها المعالج، وبالتالي كلما زادت سرعة المعالج زادت قدرته على التعامل مع عدد تعليمات أكبر في وقت أقل، وبالتالي تنفيذ مهامك بشكل أسرع.

في الغالب تكون السرعة المحددة على أي معالج هي سرعة كل نواة على حدة في حال كان المعالج متعدد الأنوية.

عدد الأنويةCores

قديمًا كان المعالج يحتوي على نواة واحدة فقط تقوم بكل الأعمال وحدها، ولكن مع تطور التطبيقات والحاجة لعمل العديد من المهام في نفس الوقت الأمر أصبح المعالج مع الوقت هو المتهم الأول في حدوث أي بطء أو تأخير. لذا، ظهر الحل البسيط: إضافة المزيد من الأنوية!

الأنوية ببساطة تعتبر معالجات إضافية، نحن لا نتحدث هنا عن معالج أصبحت سرعته الضعف، ولكننا نتحدث عن معالج أصبح لديه القدرة على العمل بسرعةٍ كاملة لتنفيذ مهمة ما، بينما يظل قادرًا على تنفيذ عدد من المهمات الأخرى بنفس السرعة والكفاءة مستخدمًا في ذلك الأنوية الأخرى المتاحة.

المثير في موضوع عدد الأنوية هو عدم ظهور فعاليته الحقيقية إلّا عندما يكون التطبيق أو البرنامج قيد التشغيل مصمم خصيصًا ليستغل تلك الخاصية بالشكل الأمثل. لذا، لن تجد فارقًا ملحوظًا في الأداء بين المعالجات متعددة النواة وأحادية النواة في إدارة التطبيقات القديمة، لربما وجدت تلك التطبيقات تعمل بشكل أفضل على المعالجات القديمة كذلك!

الكثير يعتمد على هاتين الخاصيتين فقط عند الرغبة في شراء معالج جديد، فهل تظن أنّ ما سبق كافيًا لتصبح قادرًا على اتخاذ القرار بشراء معالج ما؟ إذا كانت إجابتك بنعم فأرجو منك الإجابة على السؤال التالي:

معالج Intel Core i7-6700K سرعته ٤ GHzوعدد الأنوية به ٤ أنوية.

معالج AMD FX-8350 سرعته ٤ GHzوعدد الأنوية به ٨ أنوية.

من الأفضل؟

الإجابة: معالج ... Intel وبفارق كبير!

كيف ذلك ؟؟ الإجابة ببساطة هي أنّ الحكم على أداء المعالج يتجاوز مسألة سرعته أو عدد أنويته، فلنكمل معًا الحديث لتوضيح الأمور بشكل أكبر.

مجموعة المنتج / Product Groups / Product Lines Modifiers

أي عدد من المعالجات يتشابه في الاسم والغرض من التصنيع يمكن تمثيله في مجموعة واحدة، فمثلًا مجموعة معالجات Xeon كانت مصممة للعمل في السيرفراتServers ، بينما معالجات Core i7 Mobileصممت للعمل مع الأجهزة المحمولة مثل الـLaptop.

إليكم عدد من المجموعات التي ربما تكون مألوفة لديكم:

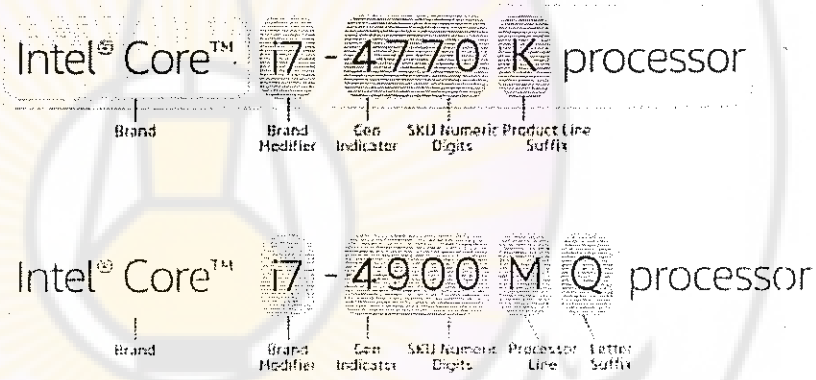
- Core i3

- Core i5
- Core i7
- Core i9
- Core i5 Mobile
- Core i7 Mobile
- Xeon

كذلك في معالجات AMD يوجد:

- A-Series
- FX
- Opteron 6200

كود المعالجCode



هو الذي يحدد مواصفات كل معالج من المعالجات المندرجة تحت مجموعة معينة، فنجد مثلًا Core i7-5960X و... Core i7-5930K الكود الذي يلي Core i7 يحدد خصائص كل معالج من حيث الجيل الذي ينتمي له، واستهلاكه للطاقة وإمكانية كسر سرعته الأصلية

المدخلSocket

هو ببساطة المكان المخصص لتركيب المعالج على اللوحة الأم، حيث لا يمكن تركيب أي معالج إلّا في الـ Socket المخصص له.

في حالة معالجات Intel يعبر اسم الـ Socket عن عدد الدبابيس pins بين المعالج واللوحة الأم، فمثلًا Intel socket 1155 يعبر عن وجود ١١٥٥ pin بين المعالج واللوحة الأم بينما Intel socket 2011يعبر عن وجود ٢٠١١ ... pin وهكذا.

تستخدم معالجات AMD تسمية مختلفة للـ Socket مثل AM4 و+AM3 ، فقط احذر جيدًا عند شرائك أي معالج وتأكد من أنّه يحمل نفس نوع الـ Socket الذي تدعمه اللوحة الأم الخاصة بك!

تكنولوجيا العمليةProcess Technology

ربما قرأت عن المعالجات التي تم تصميمها بتكنولوجيا ٣٢ nmعلى سبيل المثال، لنقل – وبدون الدخول في تفاصيل – أنّه كلما قل هذا الرقم كلما كان هذا يعني أنّ عملية التصنيع كانت (أصغر) وهذا أمر رائع؛ لأنّه يعني وجود مساحة أكبر لإضافة المزيد من المكونات للمعالج، بالإضافة لاستهلاك طاقة أقل.

هذا يوضح السبب وراء كون معالجات اليوم هي الأصغر والأقوى على الإطلاق. لنأخذ أكبر الأرقام وهو ٣٢nm، يكفي أن تعرف أنّ قطر شعرة من رأسك أكبر من هذا الرقم بأكثر من ٣٠ ضعف

خاصيةHyperthreading

المعالجات الداعمة لهذه الخاصية تخدع نظام التشغيل وتقنعه بأنّها تمتلك ضعف عدد الأنوية الموجودة حقيقةً، فمثلًا معالج ذو ٤ أنوية سيراه نظام التشغيل معالج ذو ٨ أنوية .. وهكذا، مما يعزز – وبشدة – قدرة المعالج في العمل في مهام متعددة في نفس الوقت.Multi-tasking

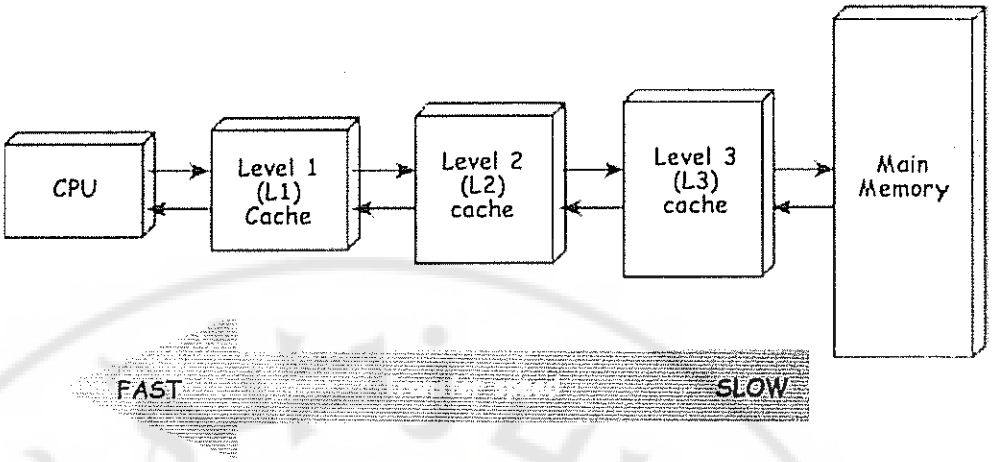
تميل المعالجات دائمًا إلى إنهاء المهمة التي تعمل عليها تمامًا قبل البدء في مهمة جديدة، أمّا في حالة دعم المعالج لخاصية Hyperthreading فإنّ هذا يعطي لأي نواة القدرة على البدء في مهمة جديدة في حال توقف المهمة الحالية لأي سبب، خاصية هامة ولكن لن تحتاجها إذا كان استخدامك للحاسب استخدام طبيعي مثل تصفح الإنترنت وخلافه.

خاصيةTurbo Boost / Turbo Core

وفيها يزيد المعالج من سرعته بشكل مؤقت حال ظهور الحاجة لذلك.

ذاكرة المعالجCache

هي ذاكرة مؤقتة تشبه الذاكرة المثبتة في اللوحة الأم RAM ولكنها أصغر بكثير وتتواجد في المعالج نفسه، وسر أهميتها هو أنّ المعالج يصل إليها بشكل أسرع بكثير من الـRAM ، ويمكن اعتبارها من الخصائص المؤثرة جدًا في سرعة المعالج عند العمل مع مهام متعددة كثيرة في نفس الوقت.



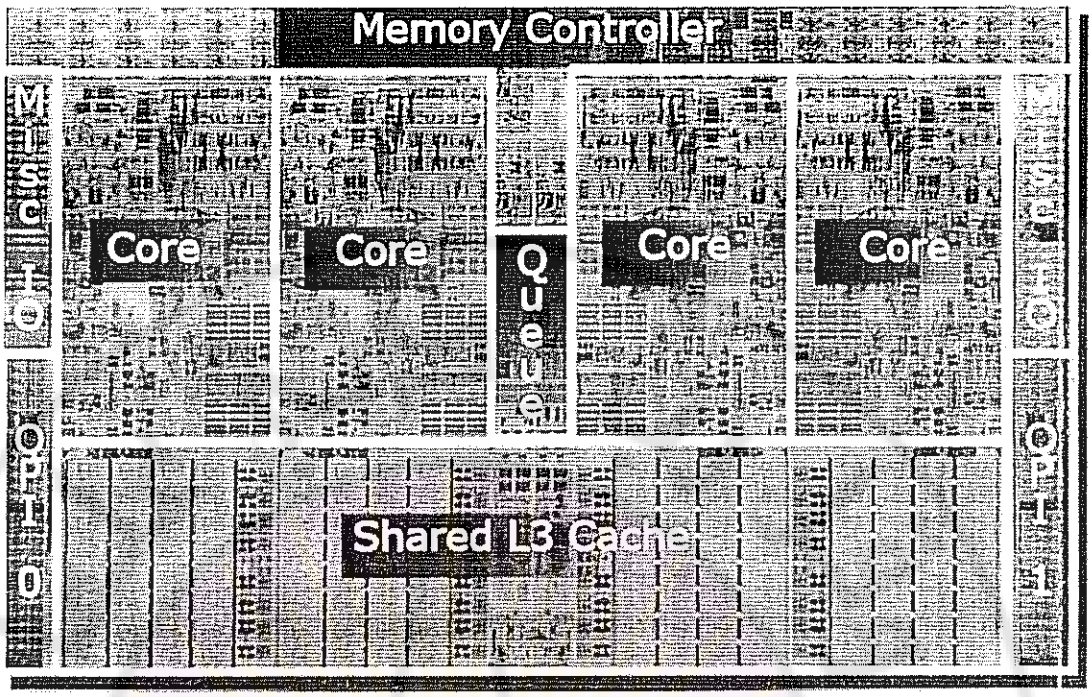
يتم تقسيم الـ cache لعدد من الطبقات Levels وهم في الأغلب طبقتان أو ثلاثة، يُشار إليهم اختصارًا بالرموز L1 و L2 و L3.

تقسيم الـ cache لطبقات بدلًا من ذاكرة واحدة كبيرة يرجع لسبب بسيط، وهو أنّه كلما زادت مساحة الـ cache زادت البيانات التي يمكن تخزينها فيه، وزاد معها الوقت الذي سيبحث فيه المعالج عن تلك البيانات عند الاحتياج إليها.

الطبقة الأولى من المعالج L1 cache هي أول طبقة يبحث فيها المعالج عن أيّة بيانات، وهي أصغر الطبقات مساحة وبالتالي هي الأسرع.

الطبقة الثانية من المعالج L2 cache هي المكان التالي الذي يبحث فيه المعالج عن أيّة بيانات، مساحة هذه الطبقة أكبر من الأولى ولكنها أبطأ لنفس السبب!

كل نواة في المعالج تمتلك طبقتي cache ، وفي حال وجدت طبقة ثالثة L3 cache تكون مشتركة بين الأنوية وتكون ذات مساحة أكبر بكثير من الطبقتين السابقتين وأبطأ أيضًا، ولكنها على الرغم من ذلك أسرع من الذاكرة RAM بكثير!



وكما يتضح لنا أنّه ليس بالضرورة أنّ قيمة cache أكبر تعني أداءً أفضل وأعلى، إلّا في حالة L3 cacheالتي لا تهتم بالسرعة كثيرًا لأنّها كبيرة للغاية.

أجيال معالجات Intel

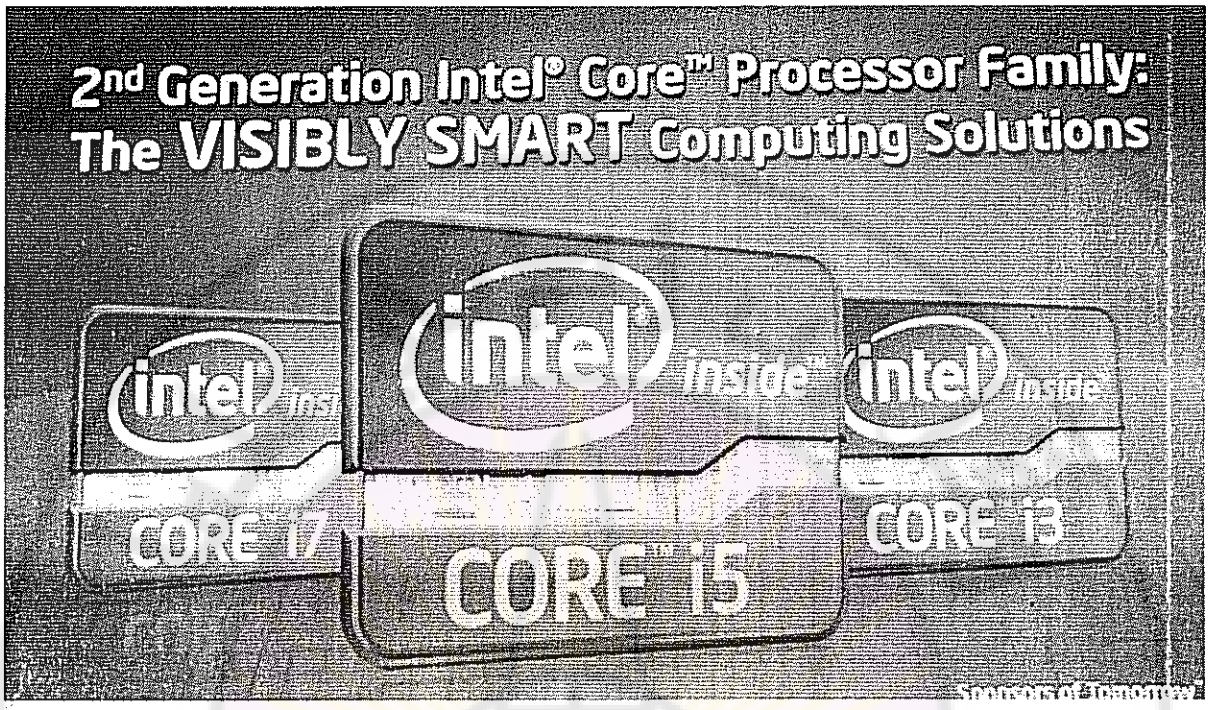
الجيل الأول Nehalem

صدر هذا الجيل في نوفمبر ٢٠٠٨ بمعالجات Core i3 و Core i5 و Core i7 ، وقدمت تكنولوجيا ٤٥ nmبخلاف المعالجات السابقة لها، والتي كانت تعمل إمّا بتكنولوجيا ٦٠ nmأو ٩٠ nm.

المعالجات من هذا الجيل كانت تمتلك L1 cache بقيمة ٦٤KB، وكذلك L2 cache بقيمة ٢٥٦KB، وأخيرًا L3 cache بقيمة تتراوح من ٤ MBإلى ١٢ MBتتشارك فيها كل الأنوية كما وضحنا سبقًا.

المعالجات في هذا الجيل تستخدم الـ Sockets الآتية: LGA 1156 ، rPGA-988A BGA-1288 ، LGA 1366

الجيل الثاني Sandy Bridge



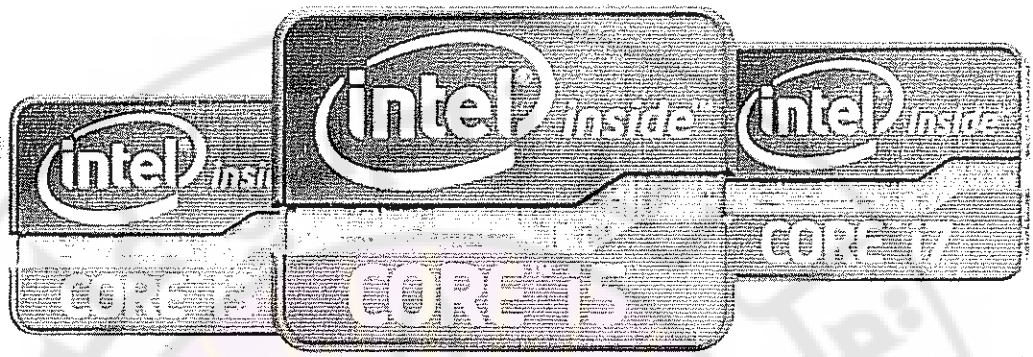
صدر في بداية ٢٠١١ بمعالجات Core i3 و Core i5 و Core i7 أيضًا ولكن بطريقة جديدة لتوضيح موديل المعالج، وقدمت تكنولوجيا ٣٢ nmبخلاف الجيل السابق لها والذي كان يعمل بتكنولوجيا ٤٥.nm

المعالجات من هذا الجيل كانت تمتلك L1 cache بقيمة KB٦٤، وكذلك L2 cache بقيمة KB٢٥٦، تمامًا مثل Nehalem ولكنها تمتلك L3 cache بقيمة تتراوح من ١ MBالى ٨.MB

المعالجات في هذا الجيل تستخدم الـ Sockets الآتية: LGA 1155 ، rPGA-988B BGA-، LGA 2011، 1023

الجيل الثالث Ivy Bridge

3rd Generation Intel® Core™ Processor Family



صدر هذا الجيل للحواسيب المحمولة Laptops في أبريل ٢٠١٢ وللحواسيب المكتبية Desktops في سبتمبر ٢٠١٢، وقدمت تكنولوجيا ٢٢ nmبخلاف الجيل السابق لها والذي كان يعمل بتكنولوجيا ٣٢ nm.

لربما كانت المشكلة الوحيدة في هذا الجيل هو انبعاث كمية حرارة أكبر منه مقارنة بالجيل السابق له.

المعالجات في هذا الجيل تستخدم الـ Sockets الآتية: LGA 1155 ، rPGA-988B BGA-1023، LGA 2011

الجيل الرابعHaswell

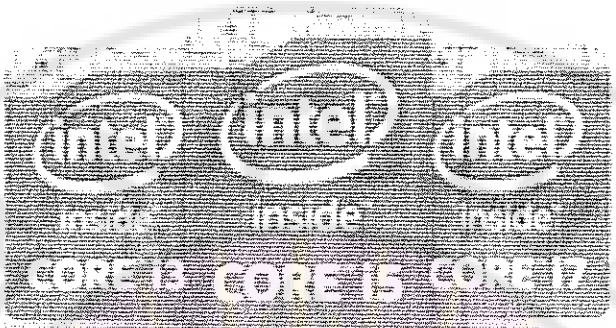
بتطور في الأداء يصل إلى ٨% عن الجيل الثالث، صدر هذا الجيل في ٢٠١٣ بنفس تكنولوجيا ٢٢ nm مع ظهور sockets جديدة لهذا الجيل مثل.LGA 1150, BGA 1364, LGA 2011-3 :

هذا الجيل كان له استخدامات كبيرة في الأجهزة المحمولة نظرًا لتوفيره الهائل في الطاقة.

المعالجات في هذا الجيل تستخدم الـ Sockets الآتيةLGA 1150 : ،BGA 1364 BGA 1168 LGA 2011-3، Socket G3،

الجيل الخامسBroadwell

5th Gen Intel® Core™ Processors

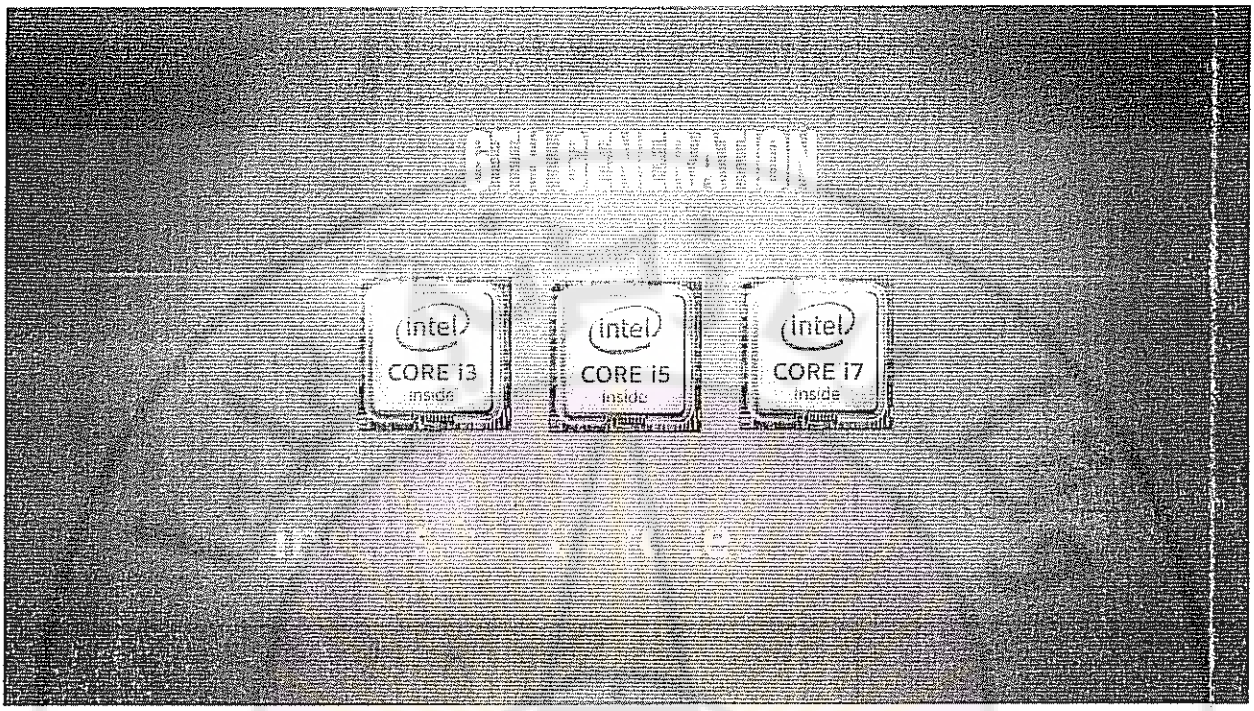


Power to transform the way you compute

صدر في ٢٠١٤ واستمر في الصدور حتى ٢٠١٥ مع تطور كبير في التكنولوجيا المستخدمة لتصبح ١٤ nmفقط! هذا التطور صحبه تطور منطقي في أداء الحواسيب المحمولة وبالطبع الحواسيب الشخصية.

المعالجات في هذا الجيل تستخدم الـ Sockets الآتية: LGA 1150، BGA 1168 Socket G3، BGA 1234، LGA 2011-3،

الجيل السادسSkylake



صدر في أغسطس ٢٠١٥، تم تصميمه على نفس التكنولوجيا السابقة ١٤nm، ولكنه على الرغم من ذلك يتفوق في الأداء مع استهلاك طاقة أقل، وأصبحت المعالجات التي تحمل حرف k في نهايتها هي فقط القابلة لأن يتم كسر سرعتها.

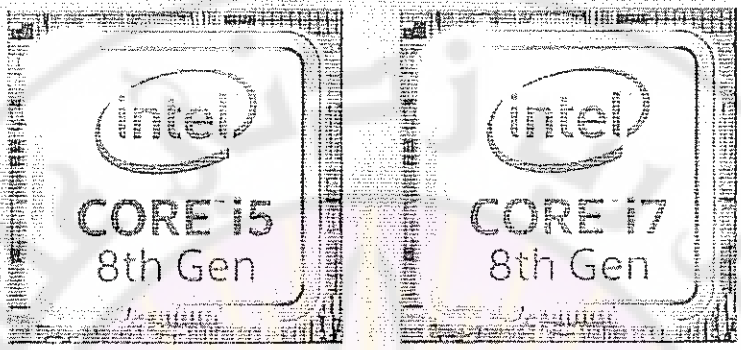
المعالجات في هذا الجيل تستخدم الـ Sockets الآتية: LGA 1151، FBGA 1356

الجيل السابعKaby Lake

صدر في أكتوبر ٢٠١٦ للحواسيب المحمولة وأوائل ٢٠١٧ للحواسيب المكتبية بتكنولوجيا ١٤ nmهو الآخر، ولكن بسرعات معالجة Clock Speeds أعلى، وكذلك Turbo Boost أعلى، مع تعديلات طفيفة على معمارية Skylake السابقة، لتعطي أداءً أفضل مع الجرافيك والعروض ذات دقة k٤، ولأول مرة يمكنك كسر سرعة معالجات من النوع.Core i3

المعالجات في هذا الجيل تستخدم الـ Socket الآتي فقط للأجهزة المكتبية: LGA 1151

الجيل الثامنCoffee Lake / Cannon Lake



حيث أعلنت Intel عن إصدارها الجيل الثامن من معالجاتها كالعادة أولًا للأجهزة المحمولة، وذلك قبل نهاية عام ٢٠١٧ كرد فعل على الإصدار الناجح جدًا من AMD والذي يحمل الاسم.Ryzen

:ما تم الإعلان عنه أو ما تم حتى تداوله على سبيل الإشاعات المتوقع – وبشدة – أن تصيب كان كالآتي

- مضاعفة عدد الأنوية في معالجات الحواسيب المحمولة.
- زيادة في السرعة عن الجيل السابع تصل إلى ٤٠.%
- معمارية Cannon Lake سوف تعتمد تكنولوجيا ١٠ nmبينما Coffee Lake ستعمل على تكنولوجيا ١٤ nmمحسّنة.
- لا توجد معلومات كافية عن جيل Coffee Lake الموجه للحواسيب المكتبية Desktops بعد.

تم الإعلان عن أربعة معالجات من هذا الجيل وهم i7-8650U :، i7-8550U، i5-8350U،-i5 8250U.

جميع المعالجات رباعية النواة، موجهة للحواسيب المحمولة، وتعتمد في معماريتها على معمارية الجيل السابع Kaby Lake architecture ولكنها معدّلة ومحسّنة، على أن تصدر معالجات من معمارية Cannon Lakeللحواسيب المحمولة قبل نهاية هذا العام.

يبدو أنّ اقتراب AMD من حيز المنافسة بعد معالجات Ryzen كان حافزًا كبيرًا لـ Intel كي تقوم بهذه الخطوة، والتي نتوقع أن تُحدث تطورًا كبيرًا خاصةً في عالم الحواسيب المحمولة، فلأول مرة تعتمد Intelمعمارية جديدة وفي نفس الوقت تقوم بتحسين معمارية سابقة في نفس الجيل!

نحن على كل حال في حالة تأهب قصوى لنرى ما الذي سوف يقدمه الجيل الجديد، وكيف ستتعامل AMDمع هذا الأمر.