مادة : نظم التشغيـــــــــــــل المتقدمـــة

أستاذ المادة : المهندس قديري سميـــــــــر

عدد الحصص : 05

مدة الحصـــة : 1 ساعة ونصف

الحصة الأولى : تعاريف عامة حول أنظمة التشغيل

الحصة الثانية : نظرة على تثبيت بعض أنظمة التشغيـل

الحصة الثالثـــة : نظرة على برنامج محرر النصوص وورد

الحصة الرابعة : نظرة على برنامج المجدول اكسل

الحصة الخامسة : مشاكل وحلول أنظمة التشغيل

الحصة الأولى : تعاريف عامة حول أنظمة التشغيل

نظم التشغيل System Operating :

هي عبارة عن مجموعة من البرمجيات الجاهزة و وظيفتها ضبط و إدارة التحكم بكافة الوحدات الأساسية المكونة للحاسوب وما تحتويه و هذه الوحدات من معلومات و بيانات .بالنسبة للمحاسبات الصغيرة و الكبيرة فإن نظم التشغيل لها حيز دائم في الذاكرة الأساسية لهذه الأجهزة .بينما في الحاسبات المصغرة فإن نظم التشغيل تخزن ما يسمى disks

أنواع نظم التشغيـل :

أنظمة التشغيل الثالثة الأكثر شيوعا لأجهزة الكمبيوتر هي

مايكروسوفت ويندوز - WINDOWS MICROSOFT ماك - MAC لينيكس LINUX وعادة يشغل نظام التشغيل في الجزء C من, Disk Hard ويمكن حذف نظام التشغيل واعادة تثبيته من جديد على الحاسوب.

نظام التشغيل ويناوز

صنعت مايكروسوفت نظام التشغيل ويندوز في منتصف الثمانينات. على مر السنين ، كانت هناك العديد من الإصدارات المختلفة من نظام التشغيل ويندوز هي ويندوز 11 (صدرت في عام 2015 ،)ويندوز 8(2012 ،)ويندوز 7 (2009 ،) و ويندوز فيستا (2007) وتأتي نسخة الويندوز محملة مسبقا على معظم أجهزة الكمبيوتر الجديدة، مما يساعد على جعله نظام التشغيل الأكثر

شعبية في العالم، نسبة مستخدمي ويندوز أكثر من 81 في المئة من مستخدمي انظمة التشغيل في العالم.

نظام التشغيل ماك

نظام التشغيل ماك هو من أنظمة التشغيل التي تم إنشاؤها من قبل شركة آبل. ويأتي محمل مسبقا على كافة أجهزة الكمبيوتر ماكنتوش الجديدة، أو أجهزة ماك. ومن المعروف أن جميع الإصدارات الأخيرة تعرف باسم "او اس تن"، واصداراتها الخاصة تتضمن الكابيتان صدر في 2015 يوسمايت 2014 مافريكس 2013 ماونتن ليون 2012، وليون 2011 والإحصائيات العالمية تشير الى ان عدد مستخدمي ماك تصل الى أقل من 10 ٪من عددً مستخدمي أنظمة التشغيل العالمية. وهذا الرقم قليل جدا لمستخدمي الحاسوب على مستوى العالم، وأحد أسباب ذلك هو أن أجهزة أبل تميل إلى أن تكون أكثر تكلفة. ومع ذلك، فكثير من الناس يفضلون الشكل والمظهر لنظام التشغيل الماك على ويندوز.

نظام التشغيل لينيكس

لينكس (وتنطق لينوكس) هي عائلة من أنظمة التشغيل مفتوحة المصدر، وهو ما يعني أنها يمكن تعديلها وتوزيعها من قبل أي شخص في جميع أنحاء العالم. وهذا يختلف من البرمجيات الإحتكارية مثل ويندوز، والتي يمكن تعديلها فقط من قبل الشركة التي تملك ذلك. مزايا لينكس هي أنه مجاني، وهناك العديد من الإصدارات المختلفة التي يمكنك الإختيار من بينيا .والإحصائيات العالمية تشير الى ان عدد مستخدمي لينكس يصل أقل من 2 ٪من عدد مستخدمي أنظمة التشغيل العالمية. ومع ذلك، تعمل معظم أجهزة الخوادم بنظام لينكس لأنه من السهل نسبيا ضبط خصائصه حسب الرغبة.

أقسام نظام التشغيل: تنقسم أنظمة التشغيل إلى قسمين رئيسيين حسب سماحها بتنفيذ أكثر من عملية في وقت واحدةّ أو القيام بعملية واحدة فقط في وقت معين، وأقسام أنظمة التشغيل هي :

الأنظمة المتعددة المهام ومتعددة المستخدمين :

هي الأنظمة التي تسمح بتنفيذ أكثر من عملية في الوقت نفسه وتسمح لأكثر من مستخدم باستخدام البرمجيات والتطبيقات الموجودة على الحاسب .

الأنظمة أحادية المهام وأحادية المستخدمين:

هي الأنظمة التي لا تسمح بتنفيذ اكثر من عملية واحدة في وقت واحد ولا تسمح لأكثر من مستخدم باستخدام التطبيقات المختلفة على الحاسوب .

وظائف نظام التشغيل :

- التعرف على المكونات المادية في جهاز الحاسوب
- التحكم في طريقة عمل كل جزء من هذه الأجزاء
- ادارة وترتيب المهام اثناء تشغيل الحاسوب وضمان عدم تداخلها
- الربط بين الأجزاء المكونة للجهاز وتنظيم تدفق البيانات
- المحافظة على كفاءة الحاسوب وذلك بمتابعة مكونات الحاسوب واكتشاف العيوب واصالحها
- قراءة وتنفيذ التعميمات من ذاكرة القراءة الثابتة ROM
- استلام اوامر مستخدم الجهاز
- تحميل البرمجيات التطبيقية وتنفيذ تعليماتها.

تعريف الفيروسات

تُعرّف الفيروسات الحاسوبية بالإنجليزيةComputer virus : بأنّها نوع من أنواع البرامج الضارة التي تُصمّم للانتشار من جهاز كمبيوتر إلى آخر؛ وذلك بهدف إلحاق الضرر بما تحتويه تلك الأجهزة من بيانات ومعلومات موجودة عليها أو حتّى بأنظمة تشغيلها، وينتقل الفيروس بين الأجهزة من خلال إرفاق نفسه ببرنامج أو ملف؛ حيث يبقى كامناً خلالها حتّى تهيئة الظروف المُناسبة التي تسمح له بتنفيذ أوامره البرمجية التي من شأنها إصابة الجهاز بالفيروسات، حيث أنّه عند تشغيل برنامج مُحمّل بفيروس حاسوبي؛ فإنّ الفيروس ينسخ نفسه وينتقل إلى الملفات المُخزنة أو البرامج الأخرى الموجودة عبر الجهاز.

يعود سبب تسمية الفيروسات بهذا الاسم إلى كيفية انتشارها وتكاثرها عبر الأجهزة، حيث إنّه بمجرّد إصابة أيّ ملف أو برنامج موجود عبر جهاز الحاسوب فإنّ عدوى الإصابة بالفيروس سرعان ما تنتشر وتنتقل لتُصيب الملفات والبرامج الأخرى الموجودة عبر الجهاز، والجدير بالذكر أنّ هناك شرطين رئيسيين يجب توافرهما في أيّ برنامج لكي يُعرّف على أنّه فيروس حاسوبي، وهما كالآتي:

- قدرة البرنامج على نسخ أوامره وتعليماته البرمجية في أجزاء وأماكن مُختلفة في الحاسوب.
- قدرة البرنامج على تنفيذ نفسه بشكل تلقائي عبر الجهاز، حيث إنّ الفيروسات تُنفّذ الأوامر البرمجية الخاصة بها بدلاً من تنفيذ أوامر البرامج التي تتواجد خلالها.

آلية عمل الفيروسات

يتطلّب البرنامج الفيروسي توفّر ظروف مُناسبة كي يبدأ بالعمل عبر الأجهزة، حيث إنّه بمجرّد تضمين الفيروس نفسه في أحد البرامج أو الملفات بنجاح؛ فإنّه يبقى ساكناً دون إظهار أيّة علامات أو أعراض لإصابة الجهاز بالفيروس، ولكن ما أن يُشغّل البرنامج الذي يحتوي الفيروس حتّى يبدأ تنفيذ تعليمات برنامج الفيروس بدلاً من تنفيذ تعليمات البرنامج المطلوب، وبمجرّد إصابة الجهاز فإنّ عدوى الإصابة يُمكن انتقالها من الجهاز إلى أجهزة أخرى في الشبكة.

طرق انتقال الفيروسات تنتقل الفيروسات إلى الأجهزة من خلال العديد من الطرق، ومنها الآتي:

- مرفقات البريد الإلكتروني.
- البرامج والخدمات الإلكترونية غير الرسمية.
- الملفات التي تُحمّل من الإنترنت.
- وسائط التخزين المُختلفة؛ كالأقراص الصلبة.
- الرسائل النصية عبر أجهزة الهواتف المحمولة.
- الروابط الوهمية عبر وسائل التواصل الاجتماعي المُختلفة.

أضرار الفيروسات

تُسبّب الفيروسات غالباً العديد من الأضرار لجهاز الكمبيوتر، ويجدر بالذكر أنّ تلك الأضرار تُعدّ بمثابة العلامات الدالة على إصابة الجهاز بالفيروسات، ومن هذه الأضرار الآتي:

- حذف الملفات بشكل تلقائي.
- ظهور رسائل تُشير إلى أخطاء في بعض البرامج أو الملفات التي تُشغَّل عبر الجهاز.
- بطء نظام التشغيل الذي يعمل به الجهاز، أو تجميد عمله في بعض الأحيان.
- تعطيل بعض المنافذ الموجودة عبر الجهاز.
- خطأ في عمل بعض مفاتيح لوحة المفاتيح.
- تغيير حجم الملفات الموجودة عبر الجهاز.
- تغيّر حجم الذاكرة سواء من خلال زيادة الحجم أو تقليله.
- ظهور أنشطة غير عادية عبر الجهاز؛ مثل تغيير كلمات المرور.
- ظهور النوافذ المُنبثقة بشكل مُتكرر عبر شاشة الجهاز.

خصائص الفيروسات

يُوجد العديد من الخصائص التي تمتاز بها أنواع مُعينة من الفيروسات الحاسوبية، بينما لا يتمتّع بعضها الآخر بكلّ تلك الخصائص، ومنها الآتي:

تعدّد الأشكال: تمتاز بعض أنواع الفيروسات بقدرتها على تغيير شكلها تبعاً للعديد من المُتغيرات، كما يُمكن لهذه الفيروسات تغيير طرق وصولها إلى الأجهزة المُختلفة.

التخفي: يُمكن للفيروسات إرفاق نفسها بملفات أخرى موجودة عبر جهاز الكمبيوتر، وهو ما يسمح ببقائها مُتخفيةً ضمن تلك الملفات ليتسنّى لها البدء بعملها التخريبي عبر الجهاز.

الإصابة بفيروسات أخرى: يُمكن أن تُصاب فيروسات الحاسوب بفيروسات أخرى، وذلك لأنّها مُجرّد أوامر برمجية يُمكن تعرّضها للإصابة مثلها مثل أيّ برنامج آخر موجود عبر جهاز الكمبيوتر، ويُؤدّي هذا الأمر إلى جعل الجهاز مُصاباً بأكثر من فيروس في نفس الوقت.

الديمومة: تمتاز بعض أنواع الفيروسات بقدرتها على إصابة أجزاء مُختلفة من الجهاز، وهو الأمر الذي يسمح بعودتها إليه حتّى وإن تمّت تهيئة جهاز الكمبيوتر بشكل كامل، وخاصةً إذا انتشرت العدوى للنسخ الاحتياطية التي تسترجع معلومات وبيانات المُستخدِم إلى الجهاز من خلالها.

أنواع الفيروسات :

فيروس الكتابة الفوقية (Overwrite virus) يُعتبر فيروس الكتابة الفوقية أخطر أنواع الفيروسات التي تؤثّر في الملفات الموجودة في جهاز الحاسوب؛ حيث إنّها قد تؤدي إلى إتلاف الملفات بشكل كلي وكامل، وقد تؤدّي في حال انتشارها بشكل كبير في ملفات الجهاز إلى إلحاق الضرر به وتعطيله، ويكتب هذا الفيروس الخطير فوق رمز الملف الذي يتواجد عليه الأمر في جهاز الحاسوب، ممّا يؤدّي إلى تغيير محتوى الملف بشكل كليّ أو جزئي، ويُمكن لفيروس الكتابة الفوقية أن يعمل عبر العديد من أنظمة التشغيل المُختلفة التي تعمل بها الأجهزة؛ كنظام تشغيل ويندوز، ونظام تشغيل لينكس، ونظام تشغيل ماكنتوش.

توجد طريقة واحدة للتخلّص من فيروس الكتابة الفوقية عبر جهاز الحاسوب، وهي حذف الملفات المُصابة بالفيروس بشكل نهائي ثمّ استعادتها من خلال النسخة الاحتياطية، ولهذا الفيروس أنواع شائعة منها فيروس (Grog.377)، وفيروس (Grog.202)، وفيروس (Grog.456)، وفيروس (Loveletter)؛ والذي يُعدّ أخطر أشكال فيروسات الكتابة الفوقية. فيروس الماكرو (Macro Virus) يستهدف فيروس الماكرو أجهزة الحاسوب من خلال إضافة الكود البرمجي الخاص بها إلى وحدات الماكرو الموجودة في ملفات البيانات المُختلفة؛ كالمُستندات وجداول البيانات وغيرها، ويتسبّب هذا النوع من الفيروسات في إجراء التغييرات على محتوى المُستندات المُصابة أو مسحها، بينما تصل بعض أشكال هذا الفيروس إلى حساب البريد الإلكتروني الخاص بالمُستخدِم، وتُرسل نسخاً من الملفات المُصابة إلى جميع العناوين الموجود ضمن قائمة جهات الاتصال لدى المُستخدِم.

فيروس قطاع الإقلاع (Boot Sector Virus) يُغيّر فيروس الإقلاع أو ما يُعرف بفيروس قطاع التمهيد البرنامج الخاص بإعداد عملية تشغيل جهاز الحاسوب، والذي يتمّ تخزينه في القرص الصلب الخاص في الجهاز أو عبر وسائل التخزين الأخرى كالأقراص المرنة؛ لذا فإنّه يُعتبر من أخطر الفيروسات التي قد يتعرّض لها جهاز المُستخدِم؛ وتُعتبر عملية التخلّص من هذا النوع من الفيروسات أمراً صعباً، حيث يجب مُعالجة المشكلة من خلال إعادة تثبيت نظام التشغيل بشكل كامل. انتشر هذا النوع من الفيروسات بشكل كبير في فترة التسعينيات من القرن العشرين، وذلك عندما شاع استخدام الأقراص المرنة بين مُستخدِمي أجهزة الحاسوب، وعلى الرغم من أنّ هذا النوع من الفيروسات قد يظهر من خلال محركات الأقراص المُتنقلة وفي مرفقات البريد الإلكتروني إلّا أنّ انتشاره انخفض بشكل كبير مع ظهور تحسينات في بُنية نظام الإدخال والإخراج الأساسي.

فيروس الإجراء المباشر (Direct Action virus) تكمن آلية عمل فيروس الإجراء المُباشر في الانتقال عبر جهاز الحاسوب عند النقر على الملفات القابلة للتنفيذ، والتي تكون عادةً من نوع (EXE) أو (COM)، حيث يتواجد الفيروس من خلالها، ويبدأ الفيروس عند النقر على أحد تلك الملفات بالبحث عن ملفات أخرى مُماثلة للانتقال إليها، وبدون النقر على مثل تلك الملفات فإنّ هذا الفيروس لا يُثّبت نفسه ويظل مخفياً عبر ذاكرة الجهاز، ويُعتبر هذا الفيروس من الفيروسات غير

الخطيرة، والتي لا تقوم عادةً بالتأثير الكبير على الملفات ونظام التشغيل الموجود، ويجدر بالذكر أنّ هذا النوع من الفيروسات يُمكن كشفه وإزالته بسهولة عبر استخدام برنامج مُضاد للفيروسات.

الفيروس المقيم (Resident Virus) سُمّي الفيروس المُقيم بهذا الاسم لأنّه يبقى مُقيماً بشكل دائم في ذاكرة الوصول العشوائي (RAM) الموجودة في جهاز الحاسوب، ليتخفّى ويُخزّن نفسه فيها، ويُعتبر هذا الفيروس من أنواع الفيروسات الحاسوبية الخطرة، حيث إنّه يُمكن أن يتسبّب بإصابة أيّ ملف يتمّ تشغيله في جهاز الحاسوب كونه يُحمّل وحدة النسخ الخاصة به في ذاكرة الجهاز ليكون قادراً على إصابة أيّ ملف. يتواجد للفيروس المُقيم بشكلين مُختلفين هما؛ الفيروس ذو العدوى السريعة والذي يتسبّب بأضرار بالغة على الجهاز وبشكل سريع لذا فإنّه يُمكن ملاحظة إصابة الجهاز به، والشكل الآخر هو الفيروس ذو العدوى البطيئة الذي ينتشر ببطء عبر أنحاء الجهاز دون أن يتمّ اكتشافه، وعند إصابة الجهاز بهذا النوع من الفيروسات فإنّه يصعب التخلّص منها عبر برامج مكافحة الفيروسات المُختلفة، وقد يتطلّب الأمر الاستعانة بخبير فيروسات من أجل حلّ المشكلة.

الفيروس متعدد الأجزاء (Multipartite virus) ينتشر الفيروس مُتعدد الأجزاء عبر جهاز الحاسوب بطرق مُتعددة، حيث إنّه يُحاول أن يُهاجم كلّاً من قطاع التمهيد بالإضافة إلى الملفات أو البرامج القابلة للتنفيذ الموجودة في الحاسوب، وفي حال انتقال الفيروس إلى قطاع التمهيد فإنّ الملفات الموجودة في الجهاز ستتأثر به، والعكس صحيح أيضاً فإصابة الملفات ستؤدّي إلى إصابة قطاع التمهيد ليُلحق الضرر بالجهاز، ولإزالة هذا الفيروس من الحاسوب فإنّه يتوجب إزالة جميع أجزائه التي أصابت الملفات أو التي أصابت قطاع التمهيد.

فيروس حشو الفراغ (Spacefiller virus) يُعتبر فيروس حشو الفراغ أو ما يُعرف بفيروس التجويف أحد أنواع الفيروسات النادرة في طريقة عملها، حيث إنّه يحشو نفسه ضمن أقسام فارغة من الملفات المتواجدة في جهاز المُستخدِم ودون أن يُغيّر على حجمها، وهو الأمر الذي يزيد من صعوبة اكتشافه.

الفيروس متعدد الأشكال (Polymorphic virus) يُعدّ الفيروس مُتعدد الأشكال أحد أنواع الفيروسات التي يُمكنها تغيير شكلها عند كلّ مرّة تُصيب بها ملفاً جديداً؛ لذا فإنّه يُطلق عليه أيضاً اسم فيروس التخفّي، وبالتالي يُعتبر هذا الفيروس من أصعب أنواع الفيروسات التي يُمكن لبرامج مُكافحة الفيروسات اكتشاف وجودها؛ فكلّما اكتشف برنامج مُضاد الفيروسات صنفاً من هذا الفيروس وأضافه إلى قائمته السوداء، فإنّ الفيروس يتّخذ شكلاً جديداً غير مُدرج ضمن تلك القائمة السوداء، وبالتالي يبدو كأنّه نوع جديد مختلف تماماً.

أنواع أخرى للفيروسات فيما يأتي بعض الأنواع الأخرى من الفيروسات التي يُمكن أن تُصيب جهاز الحاسوب الخاص بالمُستخدِم:

فيروس المسارات: (بالإنجليزية: Directory virus)؛ يُصيب هذا النوع من الفيروسات المسارات التي تُشير إلى مواقع الملفات عبر جهاز الحاسوب.

الفيروس المُشفر: (بالإنجليزية: Encrypted virus)؛ هو فيروس يحتوي على أوامر برمجية مُشفرة يتمّ نسخها ونقلها عبر الجهاز.

فيروس الشبكة: (بالإنجليزية: Network virus)؛ هو فيروس ينتقل عبر الشبكة المحلية التي يتصل بها جهاز الحاسوب، حيث إنّه عادةً ما يستخدم الموارد المُشتركة بين أجهزة الشبكة.
فيروس عدوى الملفات: (بالإنجليزية: File infectors)؛ هو فيروس يُصيب الملفات الموجودة عبر جهاز الحاسوب عند تحويلها إلى ملفات قابلة للتنفيذ تحمل الامتداد (exe.) وتحمل نفس الاسم الأصلي للملف.

فيروس العدوى السريعة والبطيئة: (بالإنجليزية: Fast and slow infectors)؛ هو أحد أنواع الفيروسات التي تعمل على تجنّب اكتشافها إمّا من خلال إصابة جميع ملفات النظام بشكل سريع وغالباً ما يتمّ ذلك من خلال نقل العدوى باستخدام برامج مُكافح الفيروسات نفسها؛ بحيث يتمّ نقلها عند قيام برنامج مُضاد الفيروسات بفتح أيّ ملف لفحصه، ويُمكن أن تنتشر عدوى الفيروس عبر الجهاز بشكل بطيء عند فتح الملفات أو تعديلها من قِبل المُستخدِم.

تعريف مضاد الفيروسات تُعرّف برامج مكافحة الفيروسات بأنها مجموعة البرامج التي صممت خصيصاً للكشف عن الفيروسات وإزالتها من أجهزة الحاسوب، بالإضافة إلى قدرتها على حماية أجهزة الحاسوب من مجموعة متنوعة من التهديدات كبرامج التجسس وبرامج أحصنة طروادة وغيرها من البرامج التي تعرف بالفيروسات، وقد طور العلماء برامج مكافحة الفيروسات في أواخر الثمانينات من القرن المنصرم وقد ازداد هذا التطور نتيجة لزيادة حجم المخاطر التي تهدد الحواسيب، وبعض هذه البرامج مجانية في حين أنّ بعضها الآخر مدفوع الثمن، ولكن تجدر الإشارة إلى أنّ البرامج المدفوعة الثمن من برامج مكافحة الفيروسات هي أكثر فعالية في وقاية الأجهزة وحمايتها.

مهام عمل برنامج مضاد الفيروسات

تقوم برامج مكافحة الفيروسات بمهام ووظائف متعددة، ومن أبرزها ما يلي:

- إزالة أية ملفات ذات آثار ضارة قد تدل على وجود الفيروسات.
- عمليات مسح كاملة للأجهزة، حيث تسمح هذه البرامج لمستخدميها بعمل مسوحات كاملة للأجهزة وحسب الوقت المناسب لهم.

تنظيف الأجهزة من أية برامج ضارة، حيث تقوم هذه البرامج من خلال المسوحات التي تقوم بإكتشاف وتنظيف جهاز الحاسوب من أية برامج ذات تأثير ضار، وقد تقوم بعض هذه البرامج بإزالة هذه الفيروسات تلقائياً، فيما يقوم بعضها الآخر بسؤال المستخدم عن رغبته في التخلص من هذه الفيروسات.

أمثلة على برامج مكافحة الفيروسات

توجد العديد من الشركات حول العالم التي تقوم بإنتاج البرامج المضادة للفيروسات ولمختلف أنواع الأجهزة كالحواسيب والهواتف ومن أشهر هذه البرامج هي البرامج التالية:

- Norton antivirus.
- McAfee antivirus.
- Windows Defender.
- Avast antivirus
- AVG antivirus.

طرق انتقال الفيروسات للحاسوب

قد تنتقل الفيروسات إلى أجهزة الحاسوب من خلال عدة طرق، ومن هذه الطرق ما يلي: من خلال الإنترنت، حيث يمكن أن يُحمّل المستخدم بعض الملفات التي تحوي الفيروسات. من خلال بعض أجزاء التخزين التي تحتوي على الفيروسات. من خلال العدوى من أجهزة أخرى حيث يمكن أن تنتقل الفيروسات من جهاز لآخر عبر الشبكات المحلية التي تربط الأجهزة.

مسح الفيروسات من الجهاز:

من خلال هذا المقال سيمكنكم إزالة البرامج الضارة يدويا، مثل حصان طروادة والفيروسات ومسجلات المفاتيح وبرامج الإعلانات المتسللة. وكل ذلك من خلال الويندوز أو حتى بعض الأدوات الخفيفة التي يمكن أن تسهل علينا الأمر.

اعتمادا على برمجة الفيروس أو برامج التجسس أو برامج الإعلانات المتسللة أو أي برنامج آخر غير مرغوب فيه، قد يكون من الممكن إزالته بنفسك من جهاز كمبيوتر مصاب. ومع ذلك يمكن أن تكون عملية طويلة وصعبة، ويمكن أن تلحق الضرر بملفاتك إذا لم تعمل بعض الخطوات تماما كما هو مخطط لها.

- إجراء نسخ احتياطي للمعلومات الموجودة على جهاز الكمبيوتر الخاص بك.
- استخدام برامج حماية جيدة من الفيروسات، مثل كاسبر أو أفيرا أو أفاست أو مكافي ..الخ
- القيام بمسح هذا المسار دائما، هناك الكثير من البرامج التي تمسح هذا المسار باستمرار مثل سي كلينر. **C: \ Users \ YourUserName\ AppData\ LocalLow \ Temp ****
- لكن يمكننا أن نمسحه يدويا عن طريق هذا الباتش الذي يمكنك القيام به عن طريق نسخ الكود التالي في المفكرة.

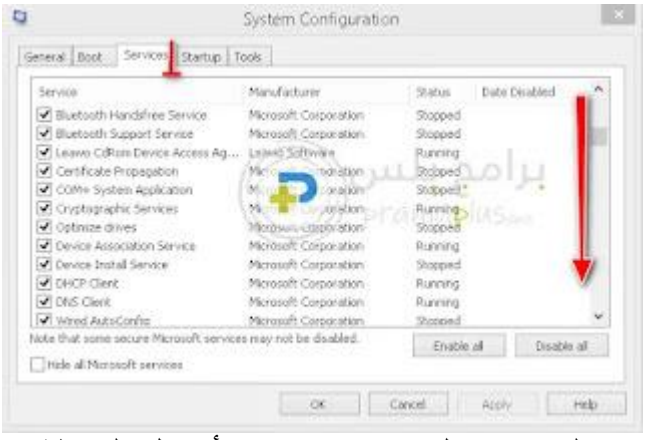
```
@echo off
del "%tmp%\*.*" /s /q /f
FOR /d %%p IN ("%tmp%\*.*") DO rmdir "%%p" /s /q
```

ثم حفظها بامتداد .bat وتشغيلها كمسئول.run as administrator

لكن بعض أنواع الفيروسات تكون محمية من المسح، لذا سنقوم بمسح الفيروسات من الجهاز بدون برامج عن طريق حذف حماية الفيروس من الويندوز.

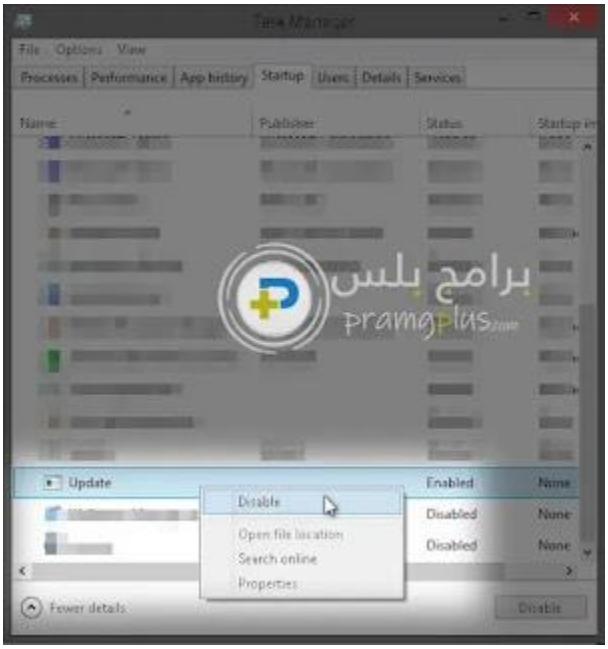
- لا يمكنك مسح الفيروسات من الجهاز بدون برامج إلا إذا وضعته في حالة خمول أولا. لذا بوضع الفيروس في حالة خمول وعدم نشاط سننهي جميع العمليات التي أنشأها الفيروس والتي تجعله قيد التشغيل.
- اكتب هذا الأمر "msconfig" في نافذةRun ، لتظهر لك كما بالصورة التالية.

وبعد الضغط على زر إنتر من لوحة المفاتيح ستظهر لنا هذه النافذة.



ستجد هنا في خدمات الويندوز كل الاتصالات والأعمال النشطة، فكل ما عليك هو حذف القيم بعدم تمكين الخدمات الغير معروفة، وكثيرا ما تكون باسم الفيروس أو اسم رسالة التحذير التي تظهر من الفيروس.

- أيضا قم بالدخول إلى مدير المهام Task manager في الويندوز وإيقاف كل البرامج الغير معلومة التي تعمل عند بدأ تشغيل الويندوز وذلك عن طريق الضغط على أزرار **CTRL +** **Shift + Esc**في نفس الوقت ليظهر لكم مدير المهام بالويندوز.
- ويمكنكم إيقاف ما تريدون من برامج تعمل مع بداية التشغيل، وللعلم ستجد الفيروس لا يحتوي على أي مسار أمامه وهذا يدل أنه برنامج غير سليم.



- لم ينتهي الأمر عند هذا الحد، حيث يمكنكم مسح الفيروسات من الجهاز بدون برامج عن طريق استخدام مدير المهام بإنهاء العمليات النشطة بالويندوز، وذلك بفتح مدير المهام ثم إيقاف العمليات النشطة، وذلك عن طريق فتح مدير المهام بالضغط على أزرار CTRL + Shift + Escفي نفس الوقت ومن ثم إلغاء مهمة الملف النشط للفيروس، يمكنك مشاهدة هذه الصورة للمزيد من المعرفة.

- مع تكرار إلغاء تنشيط ملفات الفيروس سيضحى خاملا لا قيمة له، لكنك ستحتاج إلى فحص الملفات الداخلية للجهاز، وأكثر ملفات ستجد بها الإصابة هي الملفات الخاصة بالويندوز لأنها ملفات نشطة باستمرار وإصابة الفيروس بها سيجعله عالقا في الذاكرة العشوائية بالويندوز مما يزيد من إنهاك الجهاز وازدياد فاعليته.
- قم بفتح محث الدوس CMD من خلال نافذة Run ثم الصق هذا الأمر به لإظهار كل الملفات المخفية إخفاء متقدم بالجهاز؛ لأن الفيروسات تكون مخفية إخفاء متقدم كي لا يراها المستخدم ولا يستطيع إظهارها عند قيامه بإظهار الملفات.
- اكتب اسم محرك الأقراص " C "، D، E، F، Gعلى سبيل المثال فالفيروس موجود في محرك الأقراصE ، فاكتب :E واضغط على زر إنتر.
- بعد ذلك قم بإضافة هذا النص البرمجي لإظهار جميع الملفات الموجودة

```
type attrib -s -h *.* /s /d
```

- بعد ذلك إضغط زر إنتر لتظهر لك جميع الملفات الموجودة على القسم ، سترى ملفات غريبة ذات امتدادات تنفيذية EXE ، قم بحذفها فورا.
- من أشهر الفيروسات الموجودة بالكمبيوتر هو فيروس الأوتورن، وقد لا تجد بالجهاز أي من أنواع الأنتي فيروس، وأحيانا قد لا يكون الفيروس قد سجل في قاعدة بيانات الأنتي فيروس، ولحل هذه المشكلة يمكنكم ***مسح الفيروسات من الجهاز بدون برامج*** من الفلاشة مثل فيروس الأوتورن.Autorun virus
- لذا عندما يصاب جهاز الكمبيوتر الخاص بك، قد تتصل الفيروسات سرا بموقع الويب الضار وتثبت برنامج تسجيل المفاتيح على جهاز الكمبيوتر. حيث يقوم مسجل المفاتيح بسرقة جميع معلوماتك الخاصة مثل أسماء المستخدمين وأرقام الحسابات وكلمات المرور ومعلومات بطاقة الائتمان، بالإضافة إلى معلومات حساسة أخرى. وبالتالي من المهم جدا

بالنسبة لك مسح الفيروسات من الجهاز بدون برامج من خلال فهمك لطرق تعتمد بها على نفسك عند وقوعك في أي مشكلة.

- وللقيام بإزالة فيروس autorun.inf من فلاشة USB أو الكمبيوتر اتبع هذه الخطوات.
- قم بتوصيل الفلاشة USB بجهاز الكمبيوتر الخاص بك، قد يظهر مربع حوار نافذة، لا تنقر فوق موافق ، فقط اختر "إلغاء."

- انتقل إلى موجه الأوامر واكتب حرف محرك أقراص USB الخاص بك.
- اكتب هذا الأمر dir / w / a واضغط على إنتر، سيعرض هذا قائمة بالملفات الموجودة في محرك الأقراص المحمول.

- قم بإزالة الملفات مثل Ravmon.exe ، ntdelect.com، New Folder.exe، kavo.exe svchost.exe، autorun.infإذا وجدتها.
- ولحذف الفيروس فقط اكتب del ومثال اسم الملفautorun.inf del \ :F .
- واضغط على زر إنتر من الكيبورد.
- قم بإجراء فحص لمكافحة الفيروسات على محركات أقراص USB الخاصة بك فقط للتأكد من إزالة جميع التهديدات بنجاح
- لكن يمكننا أن نمسحه يدويا عن طريق هذا الباتش الذي يمكنك القيام به عن طريق نسخ الكود التالي في المفكرة.

```
@echo on
Title HD-Boot.com
taskkill /im explorer.exe /f
taskkill /im ravmon.exe /f
start reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\EXplorer\Adva nced /v ShowSuperHidden /t
REG_DWORD /d 1 /f
start reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\RavMon"
/f
start reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared
Tools\MSConfig\startupreg\RavMon.exe" /f
start reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Run /v RavMon /f
start reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Run /v
RavMon.exe /f
start reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Run /v RavMon /f
start reg import kill.reg
if exist %systemroot%\system32\svohost.exe taskkill /f /im svohost.exe&attrib -a -s -r -h
%systemroot%\system32\svohost.exe&del /f /q %systemroot%\system32\svohost.exe
if exist c:\autorun.inf attrib -a -s -r -h c:\autorun.inf&del c:\autorun.inf
if exist d:\autorun.inf attrib -a -s -r -h d:\autorun.inf&del d:\autorun.inf
if exist e:\autorun.inf attrib -a -s -r -h e:\autorun.inf&del e:\autorun.inf
if exist f:\autorun.inf attrib -a -s -r -h f:\autorun.inf&del f:\autorun.inf
if exist g:\autorun.inf attrib -a -s -r -h g:\autorun.inf&del g:\autorun.inf
if exist h:\autorun.inf attrib -a -s -r -h h:\autorun.inf&del h:\autorun.inf
if exist i:\autorun.inf attrib -a -s -r -h i:\autorun.inf&del i:\autorun.inf
if exist j:\autorun.inf attrib -a -s -r -h j:\autorun.inf&del j:\autorun.inf
if exist k:\autorun.inf attrib -a -s -r -h k:\autorun.inf&del k:\autorun.inf
if exist l:\autorun.inf attrib -a -s -r -h l:\autorun.inf&del l:\autorun.inf
if exist m:\autorun.inf attrib -a -s -r -h m:\autorun.inf&del m:\autorun.inf
if exist n:\autorun.inf attrib -a -s -r -h n:\autorun.inf&del n:\autorun.inf
if exist o:\autorun.inf attrib -a -s -r -h o:\autorun.inf&del o:\autorun.inf
if exist p:\autorun.inf attrib -a -s -r -h p:\autorun.inf&del p:\autorun.inf
if exist q:\autorun.inf attrib -a -s -r -h q:\autorun.inf&del q:\autorun.inf
if exist r:\autorun.inf attrib -a -s -r -h r:\autorun.inf&del r:\autorun.inf
if exist s:\autorun.inf attrib -a -s -r -h s:\autorun.inf&del s:\autorun.inf
if exist t:\autorun.inf attrib -a -s -r -h t:\autorun.inf&del t:\autorun.inf
if exist u:\autorun.inf attrib -a -s -r -h u:\autorun.inf&del u:\autorun.inf
if exist v:\autorun.inf attrib -a -s -r -h v:\autorun.inf&del v:\autorun.inf
if exist w:\autorun.inf attrib -a -s -r -h w:\autorun.inf&del w:\autorun.inf
if exist x:\autorun.inf attrib -a -s -r -h x:\autorun.inf&del x:\autorun.inf
if exist y:\autorun.inf attrib -a -s -r -h y:\autorun.inf&del y:\autorun.inf
if exist z:\autorun.inf attrib -a -s -r -h z:\autorun.inf&del z:\autorun.inf
del %SYSTEMROOT%\system32\ravmon.exe /f /q /as
del %SYSTEMROOT%\system32\chostbl.exe /f /q /as
del %SYSTEMROOT%\system32\wntbhaa.exe /f /q /as
del %SYSTEMROOT%\system32\lgwubrw.exe /f /q /as
del %SYSTEMROOT%\system32\amov0.exe /f /q /as
del %SYSTEMROOT%\system32\amov01.exe /f /q /as
del %SYSTEMROOT%\system32\amov02.exe /f /q /as
del %SYSTEMROOT%\system32\funy ust scandal.exe /f /q /as
del %SYSTEMROOT%\system32\killer.exe /f /q /as
del %SYSTEMROOT%\system32\smss.exe /f /q /as
del %SYSTEMROOT%\system32\windows.exe /f /q /as
del c:\autorun.* /f /q /as
del d:\autorun.* /f /q /as
del e:\autorun.* /f /q /as
del f:\autorun.* /f /q /as
del g:\autorun.* /f /q /as
```

```
del h:\autorun.* /f /q /as
del i:\autorun.* /f /q /as
del j:\autorun.* /f /q /as
del k:\autorun.* /f /q /as
del l:\autorun.* /f /q /as
del c:\ravmon.exe /f /q /as
del d:\ravmon.exe /f /q /as
del e:\ravmon.exe /f /q /as
del f:\ravmon.exe /f /q /as
del g:\ravmon.exe /f /q /as
del h:\ravmon.exe /f /q /as
del i:\ravmon.exe /f /q /as
del j:\ravmon.exe /f /q /as
del k:\ravmon.exe /f /q /as
del l:\ravmon.exe /f /q /as
del c:\sbl.exe /f /q /as
del d:\sbl.exe /f /q /as
del e:\sbl.exe /f /q /as
del f:\sbl.exe /f /q /as
del g:\sbl.exe /f /q /as
del h:\sbl.exe /f /q /as
del i:\sbl.exe /f /q /as
del j:\sbl.exe /f /q /as
del k:\sbl.exe /f /q /as
del c:\ntdelect.com /f /q /as
del d:\ntdelect.com /f /q /as
del e:\ntdelect.com /f /q /as
del f:\ntdelect.com /f /q /as
del g:\ntdelect.com /f /q /as
del h:\ntdelect.com /f /q /as
del i:\ntdelect.com /f /q /as
del j:\ntdelect.com /f /q /as
del k:\ntdelect.com /f /q /as
del l:\ntdelect.com /f /q /as
del c:\ntldr.exe /f /q /as
del d:\ntldr.exe /f /q /as
del e:\ntldr.exe /f /q /as
del f:\ntldr.exe /f /q /as
del g:\ntldr.exe /f /q /as
del h:\ntldr.exe /f /q /as
del i:\ntldr.exe /f /q /as
del j:\ntldr.exe /f /q /as
del k:\ntldr.exe /f /q /as
del l:\ntldr.exe /f /q /as
del c:\fun.xls.exe /f /q /as
del d:\fun.xls.exe /f /q /as
del e:\fun.xls.exe /f /q /as
del f:\fun.xls.exe /f /q /as
del g:\fun.xls.exe /f /q /as
del h:\fun.xls.exe /f /q /as
del i:\fun.xls.exe /f /q /as
del g:\fun.xls.exe /f /q /as
del k:\fun.xls.exe /f /q /as
del l:\fun.xls.exe /f /q /as
del c:\oso.exe /f /q /as
del d:\oso.exe /f /q /as
del e:\oso.exe /f /q /as
del f:\oso.exe /f /q /as
del g:\oso.exe /f /q /as
del h:\oso.exe /f /q /as
```

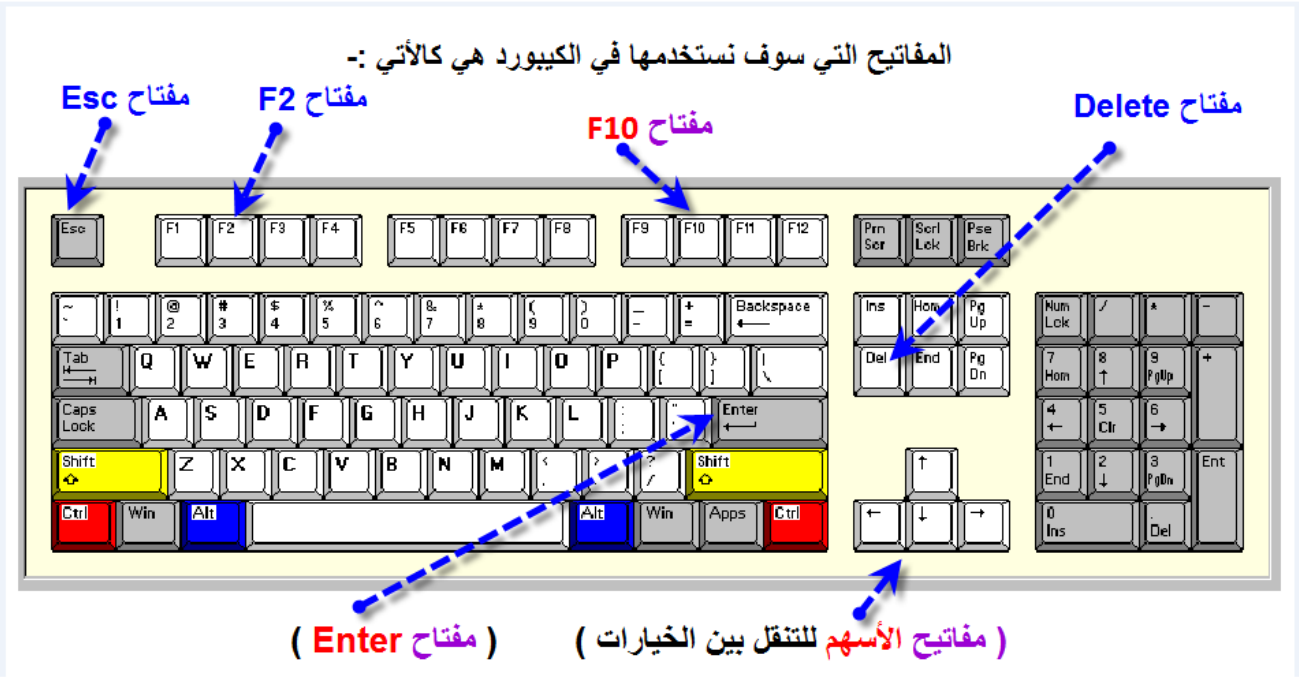
```
del i:\oso.exe /f /q /as
del j:\oso.exe /f /q /as
del k:\oso.exe /f /q /as
del l:\oso.exe /f /q /as
del c:\xdppvex.exe /f /q /as
del d:\xdppvex.exe /f /q /as
del e:\xdppvex.exe /f /q /as
del f:\xdppvex.exe /f /q /as
del g:\xdppvex.exe /f /q /as
del h:\xdppvex.exe /f /q /as
del i:\xdppvex.exe /f /q /as
del j:\xdppvex.exe /f /q /as
del k:\xdppvex.exe /f /q /as
del l:\xdppvex.exe /f /q /as
del c:\xebldqu.exe /f /q /as
del d:\xebldqu.exe /f /q /as
del e:\xebldqu.exe /f /q /as
del f:\xebldqu.exe /f /q /as
del g:\xebldqu.exe /f /q /as
del h:\xebldqu.exe /f /q /as
del i:\xebldqu.exe /f /q /as
del j:\xebldqu.exe /f /q /as
del k:\xebldqu.exe /f /q /as
del l:\xebldqu.exe /f /q /as
del c:\nideiect.com /f /q /as
del d:\nideiect.com /f /q /as
del e:\nideiect.com /f /q /as
del f:\nideiect.com /f /q /as
del g:\nideiect.com /f /q /as
del h:\nideiect.com /f /q /as
del i:\nideiect.com /f /q /as
del j:\nideiect.com /f /q /as
del k:\nideiect.com /f /q /as
del l:\nideiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del l:\usdeiect.com /f /q /as
del c:\funny ust scandal.avi.exe /f /q /as
del d:\funny ust scandal.avi.exe /f /q /as
del e:\funny ust scandal.avi.exe /f /q /as
del f:\funny ust scandal.avi.exe /f /q /as
del g:\funny ust scandal.avi.exe /f /q /as
del h:\funny ust scandal.avi.exe /f /q /as
del i:\funny ust scandal.avi.exe /f /q /as
del j:\funny ust scandal.avi.exe /f /q /as
del k:\funny ust scandal.avi.exe /f /q /as
del l:\funny ust scandal.avi.exe /f /q /as
del c:\smss.exe /f /q /as
del d:\smss.exe /f /q /as
del e:\smss.exe /f /q /as
del f:\smss.exe /f /q /as
del g:\smss.exe /f /q /as
del h:\smss.exe /f /q /as
```

```
del i:\smss.exe /f /q /as
del j:\smss.exe /f /q /as
del k:\smss.exe /f /q /as
del l:\smss.exe /f /q /as
del c:\winfile.exe /f /q /as
del d:\winfile.exe /f /q /as
del e:\winfile.exe /f /q /as
del f:\winfile.exe /f /q /as
del g:\winfile.exe /f /q /as
del h:\winfile.exe /f /q /as
del i:\winfile.exe /f /q /as
del j:\winfile.exe /f /q /as
del k:\winfile.exe /f /q /as
del l:\winfile.exe /f /q /as
del c:\comment.htt /f /q /as
del d:\comment.htt /f /q /as
del e:\comment.htt /f /q /as
del f:\comment.htt /f /q /as
del g:\comment.htt /f /q /as
del h:\comment.htt /f /q /as
del i:\comment.htt /f /q /as
del j:\comment.htt /f /q /as
del k:\comment.htt /f /q /as
del l:\comment.htt /f /q /as
del c:\80avp08.com /f /q /as
del d:\80avp08.com /f /q /as
del e:\80avp08.com /f /q /as
del f:\80avp08.com /f /q /as
del g:\80avp08.com /f /q /as
del h:\80avp08.com /f /q /as
del i:\80avp08.com /f /q /as
del j:\80avp08.com /f /q /as
del k:\80avp08.com /f /q /as
del l:\80avp08.com /f /q /as
del c:\psjqc.exe /f /q /as
del d:\psjqc.exe /f /q /as
del e:\psjqc.exe /f /q /as
del f:\psjqc.exe /f /q /as
del g:\psjqc.exe /f /q /as
del h:\psjqc.exe /f /q /as
del i:\psjqc.exe /f /q /as
del j:\psjqc.exe /f /q /as
del k:\psjqc.exe /f /q /as
del l:\psjqc.exe /f /q /as
del c:\ejlofkdo.bat /f /q /as
del d:\ejlofkdo.bat /f /q /as
del e:\ejlofkdo.bat /f /q /as
del f:\ejlofkdo.bat /f /q /as
del g:\ejlofkdo.bat /f /q /as
del h:\ejlofkdo.bat /f /q /as
del i:\ejlofkdo.bat /f /q /as
del j:\ejlofkdo.bat /f /q /as
del k:\ejlofkdo.bat /f /q /as
del l:\ejlofkdo.bat /f /q /as
del c:\xqf.*/f /q /as
del d:\xqf.*/f /q /as
del e:\xqf.*/f /q /as
del f:\xqf.*/f /q /as
del g:\xqf.*/f /q /as
del h:\xqf.*/f /q /as
```

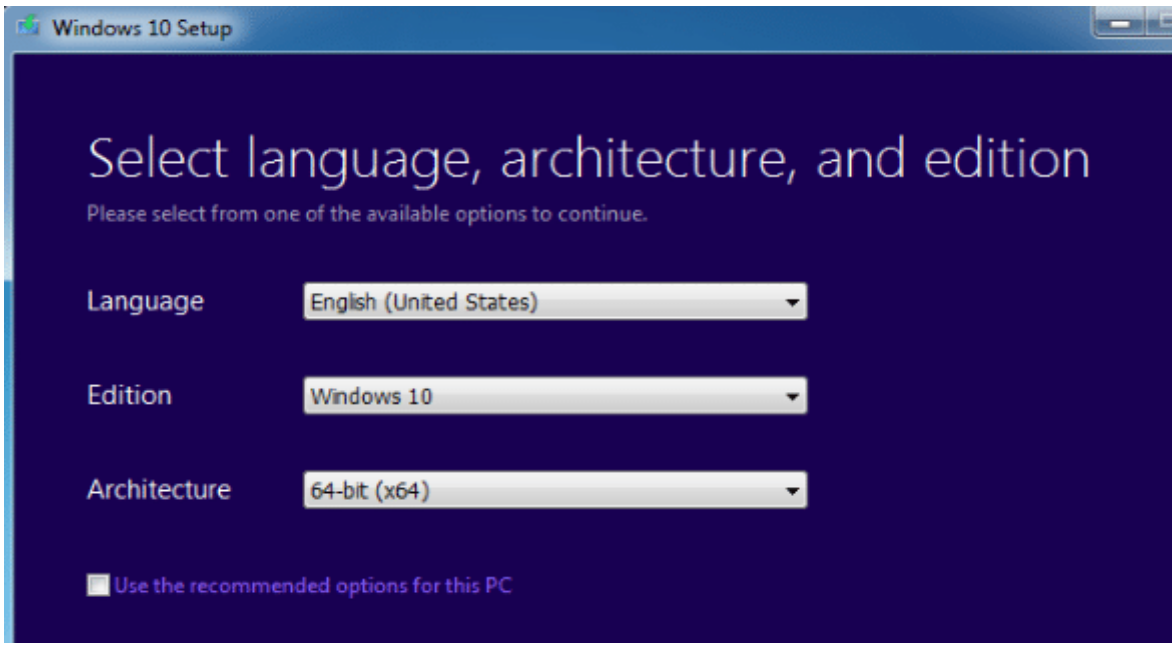
```
del i:\xqf.*/f /q /as
del j:\xqf.*/f /q /as
del k:\xqf.*/f /q /as
del c:\g1ljsm.*/f /q /as
del d:\g1ljsm *.*/f /q /as
del e:\g1ljsm.*/f /q /as
del f:\g1ljsm.*/f /q /as
del g:\g1ljsm.*/f /q /as
del h:\g1ljsm.*/f /q /as
del i:\g1ljsm.*/f /q /as
del j:\g1ljsm.*/f /q /as
del k:\g1ljsm.*/f /q /as
del l:\USBFlash.exe /f /q /as
del c:\USBFlash.exe /f /q /as
del d:\USBFlash.exe /f /q /as
del e:\USBFlash.exe /f /q /as
del f:\USBFlash.exe /f /q /as
del g:\USBFlash.exe /f /q /as
del h:\USBFlash.exe /f /q /as
del i:\USBFlash.exe /f /q /as
del j:\USBFlash.exe /f /q /as
del k:\USBFlash.exe /f /q /as
del l:\USBFlash.exe /f /q /as
del l:\USBFlash.exe /f /q /as
del c:\hklpjs.pif /f /q /as
del d:\hklpjs.pif /f /q /as
del e:\hklpjs.pif /f /q /as
del f:\hklpjs.pif /f /q /as
del g:\hklpjs.pif /f /q /as
del h:\hklpjs.pif /f /q /as
del i:\hklpjs.pif /f /q /as
del j:\hklpjs.pif /f /q /as
del k:\hklpjs.pif /f /q /as
del l:\hklpjs.pif /f /q /as
Start explorer.exe
```

ثم حفظها بامتداد bat. وتشغيلها كمسئول.run as administrator

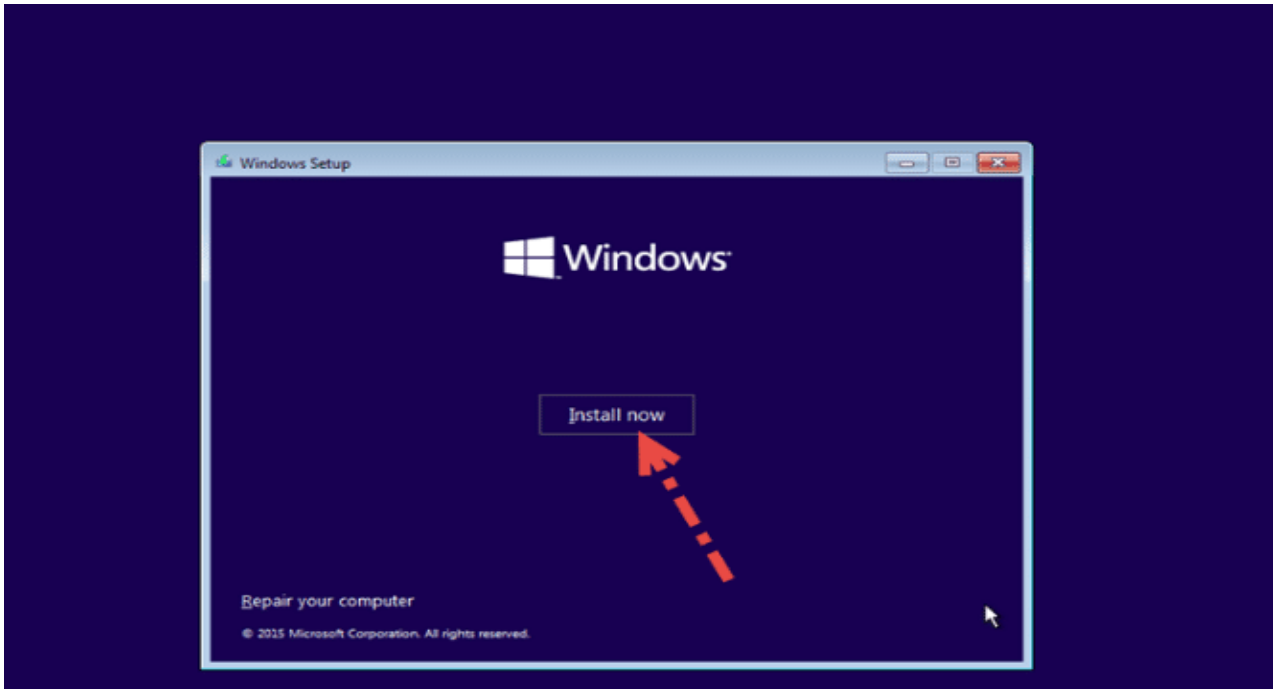
الحصة الثانية : نظرة على تثبيت بعض أنظمة التشغيـل



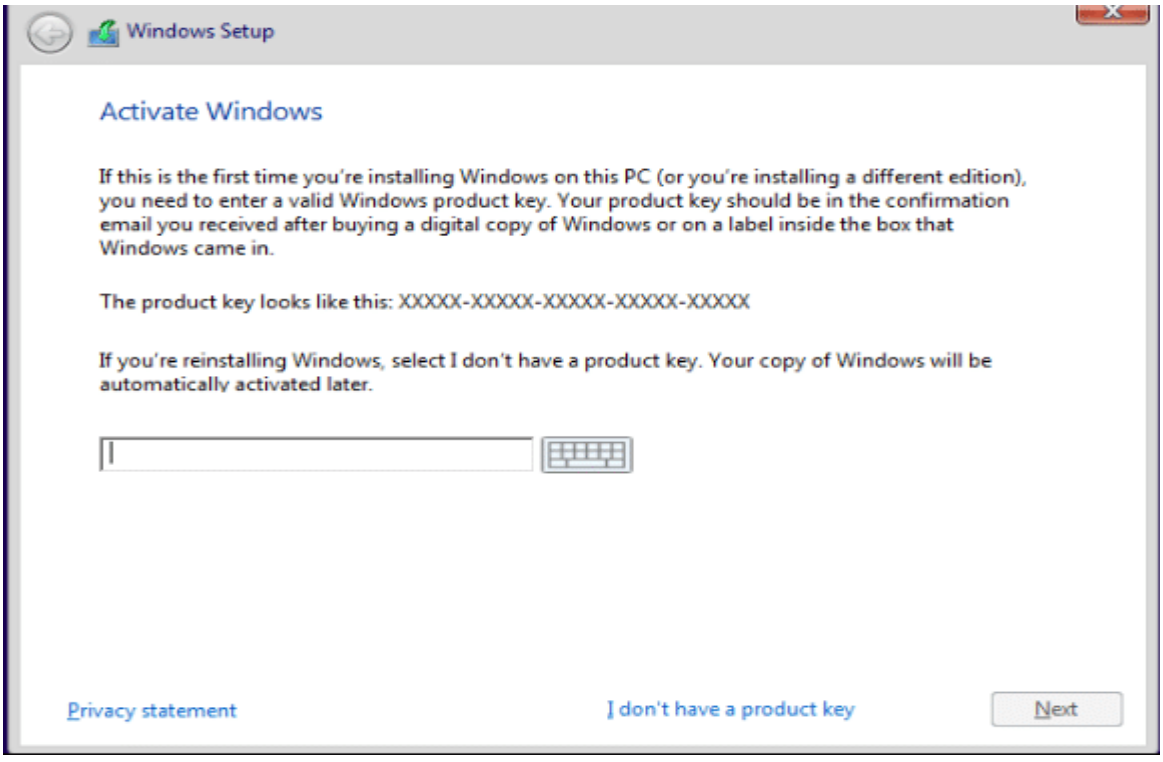
بعدما قمت بتنزيل ملفات النسخة على جهازك، قم بتحميلها على فلاشة USB أو بحرقها على إسطوانةCD ، ومن ثم قم بإدخال الفلاشة أو الـ CD بالكيسة، وأعد تشغيل الجهاز من خلال زر Restertأو إعادة تشغيل، وسيظهر لك الإعدادات الخاصة بالـ Boot (الإقلاع) وعليك أن تختار الدرايفر الذي عليه النسخة أولًا ويليه الهارد ديسك في الترتيب، وبعد هذه الخطوة سيقوم بالجهاز بعمل إعادة تشغيل تلقائيًا، ويبدأ معك أول خُطوات التنصيب. وفي الخانة الأولى عليك إختيار لغة بلدك، والخانة الثانية Edition والمقصود بها هو الإصدار الخاص بالنظام، والخانة الثالثة هى architecture والمقصود بها نوع النظام أو نمط النسخة التي تريدها ولها خيارين وهما 32 bit-أو 64(bit-، ومن ثم قم بالضغط على.Next



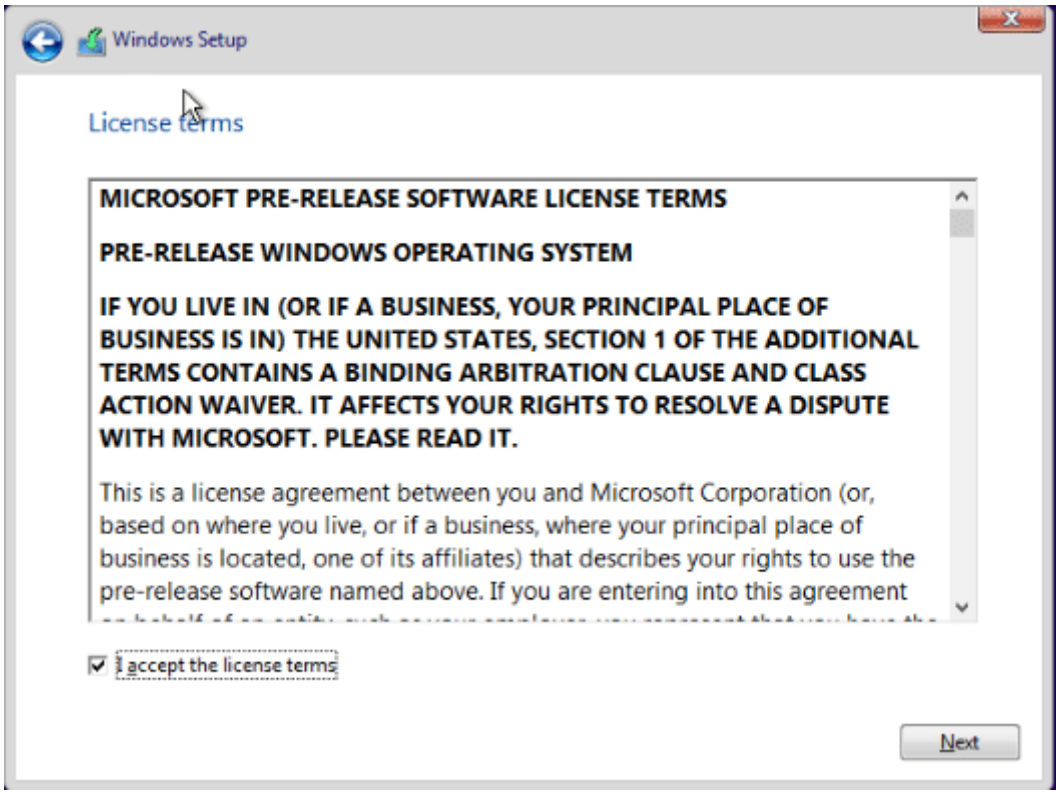
وإذا كنت تقوم بتثبيت Windows 10 على جهاز الكمبيوتر الخاص بك الحالي، فعليك أن تحرص على تحديد مربع"Use the recommended options for this PC" ، وسوف تقوم هذه الأداة بتنزيل الإصدار الصحيح لجهاز الكمبيوتر الحالي تلقائيًا.



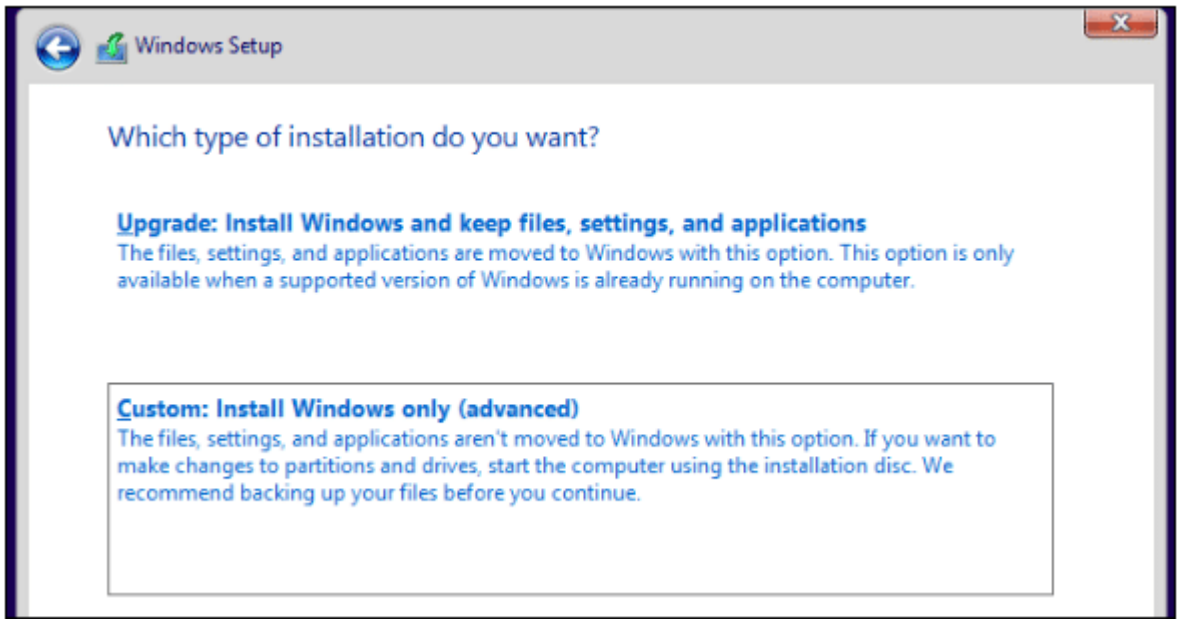
بعدها سيظهر أمامك شاشة زرقاء كما في الصورة، فعليك الضغط على.Install now



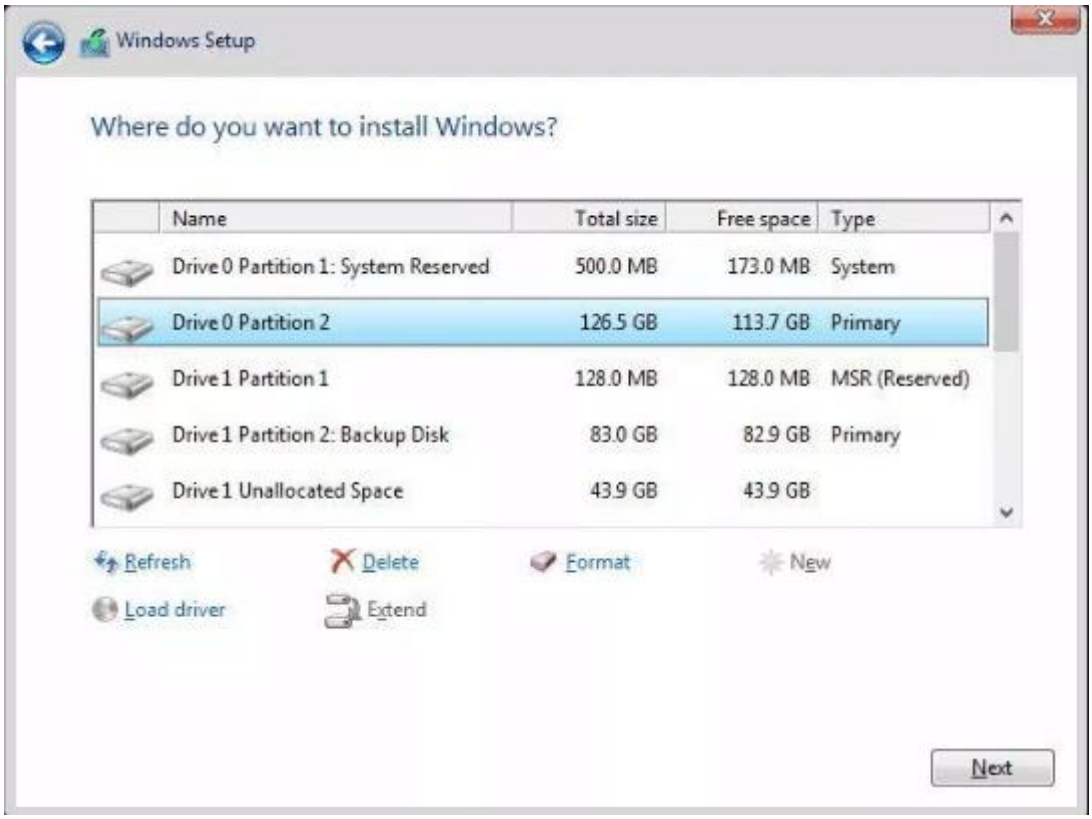
وحينما تظهر أمامك ويندوز التفعيل، فـ ستحتاج إلى إدخال مفتاح الترخيص أو يمكنك تخطيها، وقد لا تشاهد هذه الشاشة إذا اكتشف Windows 10 تلقائيًا مفتاحًا مقترنًا بجهاز الكمبيوتر الخاص بك. وفي حالة عدم تثبيت Windows 10 وتنشيطه على هذا الكمبيوتر من قبل، أدخل مفتاح Windows 10هنا. إذا لم يكن لديك واحد، ولكن لديك مفتاح Windows 7 أو 8 أو 8.1 صالح، فأدخله هنا بدلاً من ذلك. فإذا سبق لك الاستفادة من عرض ترقية Windows 10 المجاني على هذا الكمبيوتر الشخصي، فإنقر فوق "ليس لدي مفتاح منتج"، سيتم تنشيط Windows تلقائيًا بإستخدام "ترخيص رقمي" مرتبط بجهاز الكمبيوتر الخاص بك على خوادم Microsoft بمجرد تنصيبه.



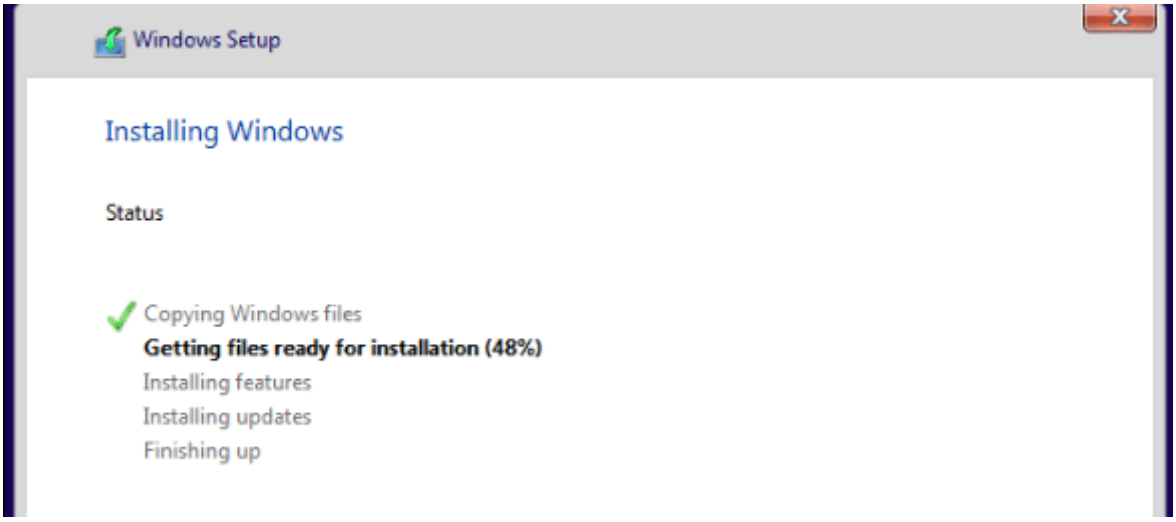
ستظهر أمامك شاشة Licence terms والتي تحتوى على شروط الترخيص، ومن ثم قم بالتحديد على مربع I accept the licence terms والنقر على.Next



عند الوصول إلى شاشة"Which type of istallation do you want" ، انقر فوق "Custom"لإجراء تثبيت نظيف وإزالة كل شيء على جهاز الكمبيوتر الخاص بك. (إذا كنت قد غيرت رأيك وترغب في ترقية التثبيت الموجود لديك، فيمكنك النقر فوق "ترقية").



ستظهر هذه الشاشة التي ستطلب منك أي قسم (برتيشن) تريد أن يتم تثبيت النسخة عليه، وغالبًا يكون البرتيشنc ، وعند إختيار لأي قسم قم بعدها بالضغط على كلمةFormat ، حتى يقوم بمحو كل الملفات الموجودة على البرتيشن الذي قمت بإختياره لينسخ ملفات جديدة للنسخة، من ثم قم بالضغط على.Next



سيقوم Windows 10 بتثبيت الملفات تلقائيًا دون تدخل منك، وقد تتم إعادة تشغيله عدة مرات أثناء هذه العملية، وعند الانتهاء سترى واجهة الإعداد العادية التي تراها عند إعداد Windows 10على أي جهاز كمبيوتر شخصي جديد، حيث يمكنك إضافة حسابات المستخدمين وتعديل الإعدادات المختلفة.