المحاضرة الرابعة

انظمة التشغيل

أنواع الفيروسات

١- الفيروسات متعددة القدرة التحويلية (مخادع): هذه الفيروسات لديها القدرة الديناميكية على تحويل وتغيير شفرتها عند الانتقال من ملف إلى أخر لكي يصعب اكتشافها .

٢- فيروسات قطاع التشغيل: تستقر هذه الفيروسات في الأماكن التي يقراها الكمبيوتر بالقرص الصلب اقلاعه (تشغيله) ليستقر في الذاكره وينفذ شفرته .

٣- فيروسات الماكرو: وهو أحدث أنواع الفيروسات وهو فيروس يكتب بلغة الورد WORDويصيب هذا الفيروس ملفات البيانات ويصيب ملفات الأوفيس.

٤- الفيروسات متعددة الملفات: يبدأ هذ الفيروس في الجهاز بصيغة أوليه ثم يتحول لصيغ أخرى ليصيب ملفات أخرى .

٥- الفيروسات الخفية : تختبئ هذه الفيروسات في الذاكره ثم تتصدى لأي طلب تشخيص وفحص قطاع التشغيل ليرسل تقريرا بأن قطاع التشغيل سليم وغير مصاب .

٦- فيروسات الملفات التنفيذية: تلصق هذه الفيروسات نفسها مع ملفات البرامج التنفيذية مثل command.comو win.com

٧- الفيروسات متعددة الاجزاء (أو متعددة المهام): يصيب هذا الفيروس قطاع الأقلاع (بدأ التشغيل) والملفات في وقت واحد

٨- فيروسات قطاع التشغيل Boot Sector: وهي أخطر أنواع الفيروسات حيث تصيب المقطع التشغيلي في القرص الصلب .

٩- الفيروسات الطفيلية: تلتصق هذه الفيروسات مع الملفات التنفيذية لتستقر في الذاكره عند عمل أحد البرامج المصابه ثم تنتظر في الذاكره إلى ان يشغل المستخدم برنامجا أخر فتقوم باصابته ونقل العدوى له .

١٠- الفيروسات المتطوره: وسميت بذلك لانها تغير شفرتها أيضا ولكن عند الانتقال من جهاز لاخر.

امثلة على بعض الفيروسات

فيروس **Brontok** أو الفيروس الذي يخفي خيارات المجلداو يفقدك التحكم في الرجستري فتصبح غير قادر على التحكم في الحاسوب: هذا الفيروس من أبرز مهامه أنه يقوم باخفاء خيارات المجلد من قائمة أدوات الموجودة في نظام الويندوز وأيضا يقوم بتكرار جميع المجلدات التي يصيبها حتى أن لاتعرف الأصل من النسخة وقد تحذف الأصل ظنا من أنه الفيروس، وهو أيضا يقوم بفتح شاشة الإنترنت اكسبلورر ويقوم بفتح شاشة خضراء اللون بشكل مستمرمما يسبب بطئ في النظام ومما يؤدي ألى زيادة انتشار هذا الفيروس في الكمبيوتر.

فيروس **xcopy** والذي يصيب ال **Partion** القسم للقرص الصلب ويجعله لا يفتح مباشرة وذلك بزرع ملف **autorun** وحينما تحاول فتح القسم يعطي قائمة فتح باستخدام ولا تستطيع الدخول إلى القسم الذي تريده إلا بطرق ملتوية مثل (استكشاف وتشغيل) للمحترفين فقط ويقوم أيضا بجعل الفلوبي دسك القرص المرن يصيح باستمرار مطالبا بادخال قرص مرن للكمبيوتر.

تصنيف الفيروسات حسب خطورتها

١- العادي : Trivial

لا يفعل الفيروس العادي شيئا سوى التكاثر replication ولا يسبب أي ضرر أو تخريب للمعلومات مثل فيروس **stupid**

٢- الثانوي : Minor

يصيب الملفات التنفيذية فقط executable file ولا يؤثر على البيانات.

٣- المعتدل : Moderate

يقوم بتدمير جميع الملفات الموجودة على القرص إما باستبدال المعلومات بمعلومات لا معنى لها أو عن طريق إعادة التهيلة Reformatting مثل فيروس **Disk killer** الذي يقوم باعادة تهيأة القرص. ويمكن حل مشكلة هذه الفيروسات عن طريق استخدام النسخ الاحتياطي.

٤- الرئيسي : Major

يؤدي الفيروس إلى تخريب المعلومات باجرا تغيرات ذكية وبارعة للبيانات دون أن يترك أثرا يشير إلى التغيير الحاصل كأن يقوم بتبديل كتل المعلومات المتساومة في الطول بين الملفات كما أن تأثيره يكون على المدى الطويل ولن يكون من الممكن اكتشاف الإصابة إلا بعد بضعة أيام وبذلك لا يمكن الوثوق بالنسخة الاحتياطية أيضا .

٥- اللا محدود : Unlimited

يستهدف الشبكات والملفات المشتركة وتمضي أكثر الوقت في محاولة معرفة كلمة السر للمستخدمين الأكثر فاعلية وعند معرفتها يقوم بتمريرها إلى أحد أو أكثر من مستخدمي الشبكة على أمل أنهم سيستخدمونها لأغراض سيئة. ترينا الفيروسات كم نحن معرضين للهجوم ولكن بالمقابل ترينا مدى التعقيد والترابط الذي وصل إليه الإنسان.

امثلة عن الفيروس اللا محدود

My doom :قدر الخبراء الحواسياب المتضررة من هذه الدودة بحوالي ربع مليون حاسوب خلال يوم واحد والذي كان في كانون الثاني ٢٠٠٤.

Melissa: أعطى هذا الفيروس فاعلية كبيرة جدا حيث أجبر شركة Microsoftوالعديد من كبرى الشركات الأخرى على إطفاء خوادم البريد بشكل كامل حتى تمكنوا من القضاء عليه وذلك في آذار ١٩٩٩

وفي الشهر الأول من عام ٢٠٠٧ ظهرت دودة اسمها Storm وبحلول الشهر التاسع كان أكثر من ٥٧ مليون حاسوب مصاب. كلنا تصور أن كل هذا التأ ير ينتج عن برامج بسيطة جدا .

لماذا يعمل الناس فيروسات الحاسوب ؟

فيروسات الحاسوب لا تتشابه في وجودها بالفيروسات الحيوية. إن فيروس الحاسوب لا ينشأ من لا شي ولا ياتي من مصدر مجهول ولا ينشأ بسبب خلل بسيط حدث في الحاسوب. فيروس الحاسوب يتم برمجته من قبل المبرمجين أو الشركات ويتم صنعه بشكل متعمد ويتم تصميمة بشكل متقن. يعمل المبرمجون على برمجة الفيروسات وذلك لاهداف عديدة تتنوع من اقتصادية وسياسية وتجارية وعسكرية. فبعض المبرمجين الهواة يعتبرون أن عمل الفيروس نوع من الفن والهواية التي يمارسونها. ومن أهم الأهداف لعمل فيروس الحاسوب هو الهدف التجاري. ذلك عن طريق عمل وصنع الفيروسات من أجل بيع برامج مضادات الفيروسات لانة بعمل الفيروس يصبح المستخدمون بحاجة إلى برامج مضادة للفيروسات ومضطرون للشراء . يذكر أن المبرمج الذي يعمل الفيروس يعتبر حسب القانون مجرما وصناعة الفيروس جريمة يحاسب عليها حسب قانون الدولة الموجود بها.

معظم شركات مضادات الفيروسات تقوم بصناعة الفيروسات من قبل المبرمجين وتقوم بعمل

مضادات لها وذلك لتسويق منتجاتها وبرامجها لدى مستخدمي الكمبيوتر. اما الأهداف العسكرية فهي محاولة الدخول لأنظمة الطرف الاخر لكشف اسرار واخذ بيانات عن طريق برامج التجسس. الأهداف الإجرامية فأهمها سرقة بيانات وارقام حسابات أو ارقام بطاقات الائتمان وكلمات السر لمحاولة الدخول لحسابات المشتركين في البنوك وسرقة اموالهم. أو سرقة بيانات من اجهزتهم.

ما هي مراحل العدوى ؟

١- **مرحلة الكمون**: حيث يختبأ الفيروس في الجهاز لفترة.

٢- **مرحلة الانتشار**: و يبدأ الفيروس في نسخ نفسه و الانتشار في البرامج و اصابتها و وضع علامته فيها.

٣- **مرحلة الانفجار** في تاريخ معين او يوم .. مثل فيروس تشرنوبيل.

٤- **مرحلة الاضرار**: و يتم فيها تخريب الجهاز

الاختراق الالكتروني (hacking)

هو قيام شخص او اكثر بمحاولة الوصول الى جهازك او الشبكة الخاصة بشركتك عن طريق شبكة الانترنت وذلل باستخدام برامج متخصصة في فك الرموز والكلمات السرية وكسر الحواجز الأمنية واستكشاف مواطن الضعف في جهازك او شبكة معلوماتك وعادة ما تكون المخارج (بوابات العبور للمعلومات) الخاصة بالشبكة المحلية وهذه اسهل الطرق للوصول الى جميع ملفاتك وبرامجك وبالنسبة للمخترقين أصبحت المهمة عسيرة بعض الشي وذلك في اختراق المؤسسات والمواقع الكبيرة بعد تطور نظم الدفاع وبرامج الحماية ولكن لأجهزة الافراد مازالت الأبواب مفتوحة.

أنواع الاختراق

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة الى ثلاثة اقسام:

١- المزودات او الأجهزة الرئيسية للشركات والمؤسسات او الجهات الحكومية.

٢- الأجهزة الشخصية

٣- البيانات

مصادر الاختراق

١- مصادر متعمده

٢- مصادر غير متعمدة

معالجة الاختراق

١- تحديث نظام التشغيل (وأفضل الطرق عبر النت)

٢- استخدام برامج مضادة للفايورسات (Antivirus) لإزالة الفايروسات وتجنب الإصابة بها.

اهم الخطوات اللازمة للحماية من عملية الاختراق

١- الحصول على جدار حماية ناري (Firewall)

٢- الحصول على برنامج مكافحة فيروسات

٣- حافظ على تحديث برامج جهازك

٤- لا تفتح رسائل البريد الإلكتروني المشكوك فيها

٥- الحذر عند إقفال النوافذ المنبثقة

٦- فكر ملياً قبل تنزيل ملفات من الإنترنت

٧- برامج مراقبة بيانات الشبكة Packet Sniffers

٨- عمل نسخ احتياطية من ملفاتك

٩- التحديثات

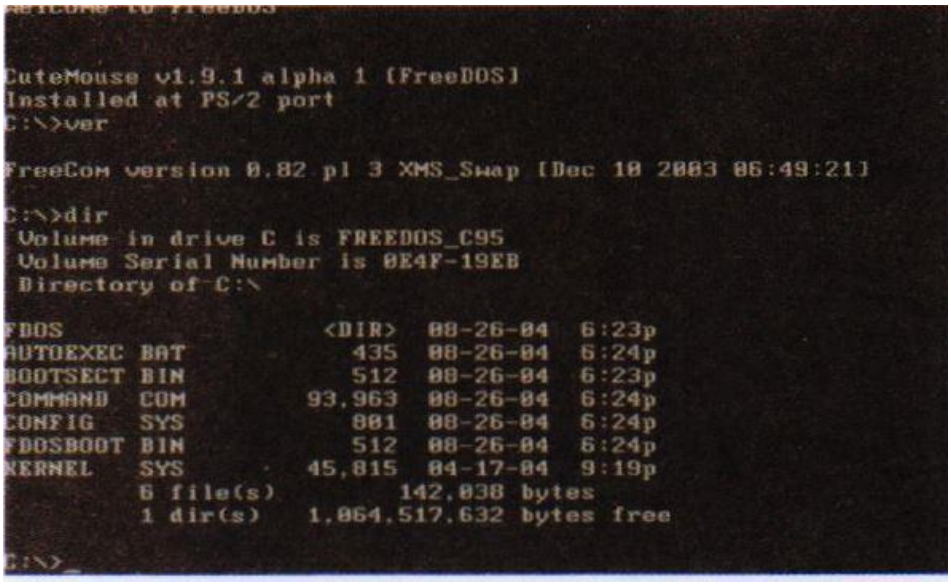
١٠- التشفير

انظمة التشغيل

١- نظام DOS للحاسوب الشخصي:

يطلق اصطلاح DOS على نظام التشغيل للحاسوب الشخصي ويعتبر من نظم ذات اسلوب الواجهة الخطية (اوامر السطر الواحد والتي تتطلب مجهود ذهني لتذكر الايعازات). وهو اختصار لـ Disk Operating System اي

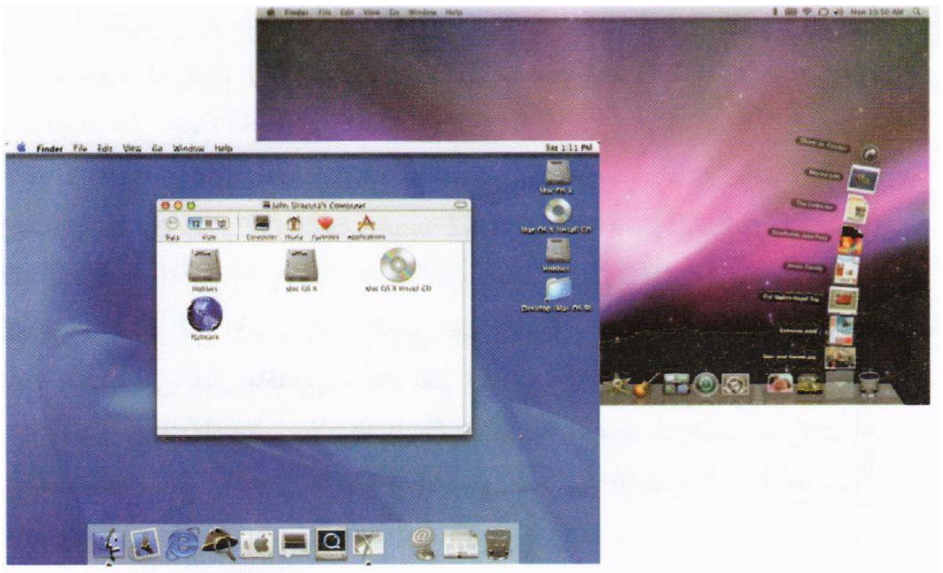
نظام تشغيل الاقراص, وقد ظهر هذا النظام عام ١٩٨١ مع الاجيال الاولى من الحواسيب الشخصية. وقد تم انتاج انواع واشكال مختلفة من نظم التشغيل هذه وحسب نوع المعالجات المتوفرة مثل Intel او Zilog وحسب الشركات المطورة, PC-DOS و MS-DOS و CPM.



شكل-١: واجهة لنظام التشغيل DOS

٢- نظام التشغيل ماكنتوش Mac OS:

تعد شركة ابل Apple اول من بدأ بالواجهات الرسومية للمستخدم GUI Graphical User Interface بالنسبة للحواسيب الشخصية حينما قدمت حواسيب ماكنتوش عام ١٩٨٤, وتطور نظام التشغيل ماك ليقدم المزيد من التسهيلات لمستخدميه في كل مرة.



شكل-٢: نماذج من واجهة نظام التشغيل ماك (Mac)

كما اصبح نظام التشغيل ماكنتوش المفضل في المكتبات التي تكون غالبية اعمالها تحرير النصوص ومعالجة الملفات وذلك للاسباب الاتية:

١- سهولة التعامل مع النظام الذي لا يحتاج الى كتابة الاوامر بل وضع مؤشر الماوس فوق التطبيق الذي يتكون من رسم بسيط واسمه.

٢- موائمة النظام للعديد من التطبيقات شائعة الاستخدام في مجالات كثيرة بمكاتب الاطباء والصحافة وبعض مجالات ادارة الاعمال.

٣- يسمح النظام بتعدد المهام لمستخدم واحد.

٤- القدرة العالية للتعامل مع الصور والرسومات.

٥- يتميز نظام التشغيل ماكنتوش بوجود تعريب متكامل للنظام منذ بدأ انتاجه وسهولة استخدامه تطبيقات الكتابة والاخراج المميز للمستندات باللغة العربية.

٦- يتيح النظام مداولات تسمح بربط اكثر من جهاز معا والاشتراك في الات الطباعة عبر شبكة خاصة لاجهزة ماكنتوش يطلق عليها شبكة (ابل تووك)

٧- سهولة اضافة اجهزة جديد للحاسوب واضافة برامجيات حديثة الى القرص الصلب.

مع سهولة ومزايا نظام تشغيل ماكنتوش, الا ان اجهزة هذا النظام تعد اقل انتشارا من الاجهزة المتوافقة مع الحاسوب الشخصي من انتاج شركة IBM وذلك نظرا لخصوصية نظام تشغيل ماكنتوش, اذ حرصت شركة ابل المنتجة له على وضعه فقط في الاجهزة التي تنتجها دون اجهزة الشركات الاخرى, وبالتالي يستطيع مستخدم اجهزة DOS والويندوز تشغيل برامجياته على اجهزة ماكنتوش.

الا ان مع تطور نظام التشغيل ماكنتوش منذ ظهور الاصدار رقم ٧,٥ مرورا بالاصدارات ٨ والاصدار ٩ ونسخته الحديثة ١٠,٥ المسماة Jaguar (النمر) و Mac OS X 10.6 Snow Leopard (فهد الجليد) صار بامكان اجهزة الماكنتوش قراءة اقراص الاجهزة المتوافقة مع نظم DOS والوندوز وبالتالي تشغيل برامجياتها على جهاز ماكنتوش, بالاضافة الى ان شركة ابل سمحت بالترخيص لشركات اخرى باستخدام نظام تشغيل ماكنتوش مما وفر في الاسواق عددا من الاجهزة المتوافقة مع نظام ابل ماكنتوش.

٣- نظام ويندوز Microsoft Windows:

تمت محاولات عديدة لتسهيل استخدام نظام التشغيل (DOS), منها المحاولات التي اضيفت بغرض استخدام تقنية حركة مفاتيح الاسهم في تسهيل عمليات التشغيل وتنظيم عرض محتويات القرص, وكذلك بتطوير برامجيات تشغيل تسمح باسلوب الواجهات والقوائم لمستخدم الحاسوب, وقد تكللت هذه الجهود بالنجاح بظهور نظام الويندوز الذي انتجته شركة مايكروسوفت الامريكية والذي يعتبر من نظم التشغيل ذات اسلوب الواجهات الرسومية, اذ يتيح استخدام تقنية الماوس والرموز الصورية.

وقد ظهر لهذا النظام عدة اصدارات منها:

١- نظام ويندوز ٣,١ (Windows 3.1) و ٣,١١ (Windows 3.11)

٢- نظام ويندوز ٩٥ (Windows 95) كنظام تشغيل متكامل

٣- نظام ويندوز ٩٨ (Windows 98)

٤- نظام ويندوز ميلينيوم (Windows ME)

٥- نظام ويندوز اكس بي (Windows XP)

٦- نظام الويندوز ٧ (Windows 7)

٧- نظام الويندوز ٨ (Windows 8)

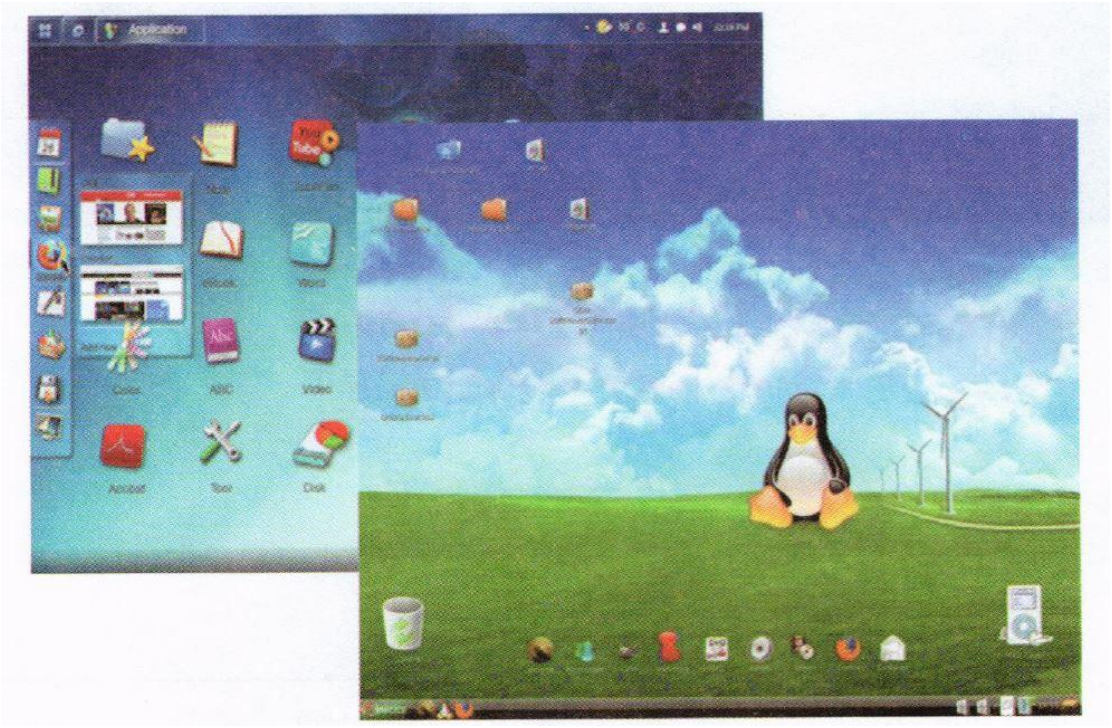
٩- نظام الويندوز ٨,١ (Windows 8.1) يستخدم بكثرة في الحواسيب او النظم التي تتطلب او تعمل باللمس (Touchscreen)

٤- نظام التشغيل ليونيكس (Linux)

هو نظام تشغيل مبني على نظام (UNIX) وهو احد اشهر الامثلة على البرامجيات الحرة وبرامجيات المصدر المفتوح (Open Source), اي انه يمكن لاي واحد ان يعدل فيه او يطور فيه ويضيف او يحذف منه اي شيء في الشيفرة الخاصة به متاحة للجميع على عكس الويندوز. من اهم مميزات هذا النظام انه يسمح بتعدد مستخدميه ويكون لكل مستخدم حساب خاص به (Account) فكل حساب له ملفاته الخاصة به ولكل المستخدمين الذين لديهم

نفس الصلاحيات. ويمتلك نظام التشغيل لينوكس بيئة رسومية (Graphical) مثل التي يستخدمها الويندوز, وكذلك بيئة نصية (Console Mode) شبيه بالـ DOS.

يتمتع لينوكس بدرجة عالية من الحرية في تعديل وتشغيل وتوزيع وتطوير اجزاءه وبسبب هذه الحرية التي يوفرها, فقد فتح المجال للاخرين للتطوير عليه بشكل نجح في التاسيس لنظام تطورة اطراف متعددة, حتى اصبح يعمل على عدد واسع من الحواسيب. وتطورت واجهات المستخدم العاملة عليه لتدعم كل لغات العالم تقريبا, وبسبب كونه حر (مفتوح المصدر) وسهولة تطويره واتاحة ذلك للجميع, فان سرعة تطوره عالية واعداد مستخدميه تتزايد على مستوى الاجهزة الشخصية والخوادم.

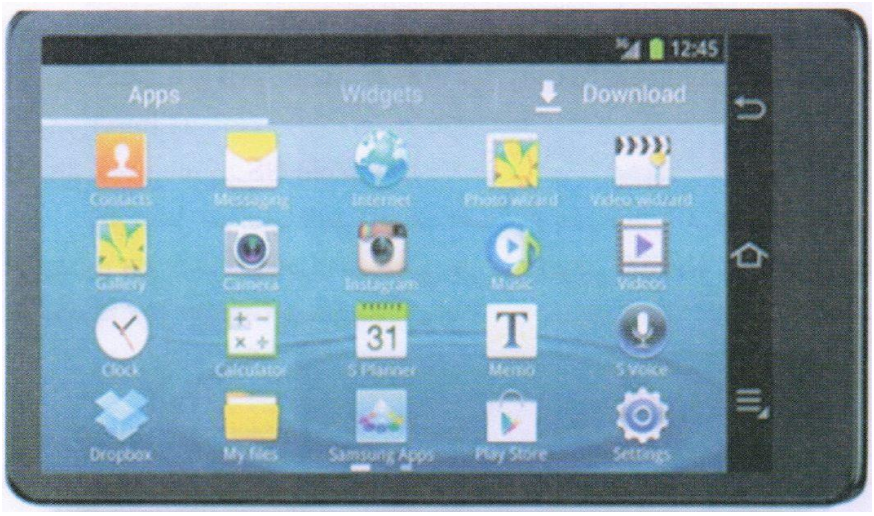


شكل-٣: واجهات نظام التشغيل لينوكس (Linux)

٥- نظام التشغيل اندرويد Android:

نظام تشغيل اعد اساسا لاجهزة الهواتف المحمولة, اذ بدات بتطويره شركة صغيرة مغمورة ليكون اول نظام تشغيل للهواتف المحمولة مبني على نواة لينوكس Linux Kernel. ولاحقا قامت شركة كوكل Google بامتلاك هذه الشركة.

وقامت تطوير نظام تشغيل جديد للهواتف المحمولة, ذات مصدر مفتوح, ويتمتع بمرونة وقابلية للتطوير هائلتين. وفي عام ٢٠٠٧ تم الاعلان عن اتحاد ضم عدد من الشركات اطلق عليه اسم Open Handset Alliance , ومن اهم اهداف هذا الاتحاد الضخم هو تشكيل ووضع مقاييس جديدة لاجهزة الهواتف المحمولة. وكان اندرويد هو اول مشروع تم الاعلان عنه من قبل هذه المجموعة.



شكل-٤: واجهات نظام التشغيل اندرويد

جدول-١ : مقارنة بين فعاليات وخواص نظم التشغيل المختلفة

Microsoft	Mac OS	Link/ UNIX	Android	iOS*	
✓	✓	✓	✓	✓	Flexible
✓	✓	✓	×	×	Multi-User
✓	✓	✓	✓	✓	Multi-Task
×	✓	✓	×	✓	Virus Protection الحماية من الفيروسات
✓	✓	✓	×	×	Windows
×	×	✓	✓	✓	Mobile
×	×	✓	✓	×	Open Source
×	✓	✓	×	✓	Secure
×	×	✓	✓	✓	Multi-touch gestures