TÖMÖRÍTÉS, VÍRUSVÉDELEM

Miért hasznos számunkra a tömörítés?

A tömörítés egy olyan eljárás, amelynek segítségével egy fájlból egy kisebb fájl állítható elő. Az adattömörítés a számítógépes tudományágak egy területe, melynek célja az adatok feldolgozása oly módon, hogy azok minél kevesebb helyet foglaljanak, vagy minél gyorsabban lehessen őket továbbítani. Ez oly módon lehetséges, hogy a valós világ adatai többnyire igen redundánsan és nem a lehető legtömörebb formában reprezentálódnak.

Mi a veszteségmentes tömörítés lényege?

A veszteségmentes tömörítés lényege, hogy az eredeti állomány kitömörítés után pontosan visszaállítódik. Ezt a tömörítési fajtát olyan esetekben alkalmazzák, ahol az adat módosulása nem engedhető meg. Ilyen helyzet áll fent például szövegfájlok, adatbázisok, programfájlok és hasonló adatok esetében. A veszteségmentes tömörítés esetén a tömörítőprogram valamilyen ismétlődéseket keres a fájlban, vagy egyéb bonyolultabb algoritmust használ az adathalmaz kisebbé tételére. Veszteségmentesen tömörített adatok fájlkiterjesztései pl.: .zip .rar .arj.

Mi a veszteséges tömörítés lényege?

A veszteséges tömörítés lényege az, hogy bizonyos nem fontos információkat a tömörítőprogram elhagy a fájlból, így annak mérete kisebb lesz. Azonban ilyen tömörítésnél az információ nem állítható vissza tökéletesen. Ez megengedhető kép, hang illetve videofájloknál.

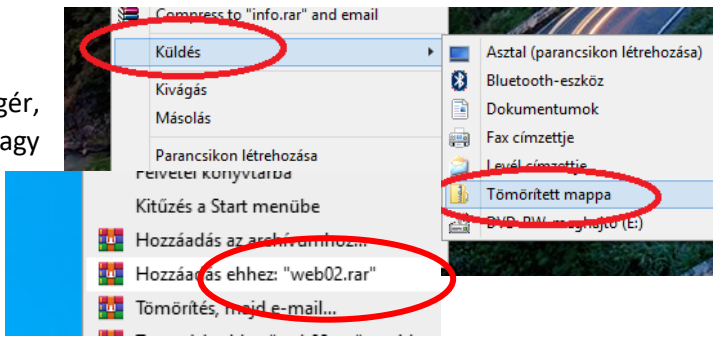
Kép tömörítésénél az eljárás állhat az egymás mellett lévő képpontok átlagolásából illetve a színmélység csökkentéséből stb. Veszteségesen tömörített képfájl-kiterjesztések pl.: jpg, png, gif.

A hang tömörítésénél általában a mintavételezési frekvenciát és a bitrátát csökkentik. Azonban felhasználják az emberi fül hibáit is, pl.: bizonyos frekvenciatartományokat kiszűrnek a zenéből (ultrahangok, infrahangok) illetve erős basszusrész után bizonyos tartományokra kevésbé érzékeny a fül, így azokat is eltávolítják a kodekek. Ilyen formátumok pl.: mp3, ogg , wma.

A videó tömörítésénél az előbb leírt eljárásokat kombinálják a kép és a hang tömörítésére. Azonban kiegészítik még az fps (frame per sec – kép per másodperc) szám csökkentésével, kihasználva a szem tehetetlenségét. Tömörített videó-formátumok pl.: avi, wmv, mpeg, mov (Quicktime)

Hogyan tömörítünk a gyakorlatban veszteségmentesen?

A tömörítendő mappán, vagy fájlokon jobb egér, majd „küldés”, „Tömörített mappa” (zip), vagy „Hozzáadás ehhez…” (rar).



Hogyan csomagoljuk ki a veszteségmentesen tömörített fájlokat?

A tömörített fájlon, „Kibontás ide”!

02/9. GYAKORLATI FELADAT

1.) Hozzál létre az asztalon egy Képek nevű mappát!
2.) Mentsél ebbe a mappába négy, - minden egyes évszakra jellemző – jpg képet!
3.) Majd az asztalon lévő mappát tömörítsd RAR formátumba!
4.) Aztán nevezd át ezt a fájlt „Évszakok”-ra!
5.) Helyezd át a tömörített fájlt egy másik adattároló eszközre (pl. pendrive-ra)!
6.) Végül bontsad ki a fájlt ott helyben!

Mi az a számítógépes vírus, féreg?

Számítógépvírusnak az olyan programokat nevezzük, amelyek a rendszerbe engedély nélkül lépnek be, önmaguk másolására, többszörözésére, és más programok megfertőzésére képesek. A vírusok többsége ezen kívül valamilyen esemény hatására, vagy egy előre meghatározott időpontban aktiválódva még más károkat is okozhat az állományainkban.

Hogyan kaphatunk vírust?

A vírus nem terem és nem fejlődik ki magától. Ahhoz, hogy vírus kerüljön a számítógépünkre, valamilyen adatátviteli eszköz használata szükséges, mint például a hajlékonylemez, merevlemez, cserélhető adattároló (pendrive, CD, stb.) vagy egy hálózati kapcsolat (internet).

Melyek a figyelmeztető jelek?

Ha a gépünkön valamilyen megmagyarázhatatlan rendellenességet tapasztalunk, vírusfertőzésre kell gyanakodnunk.

Ilyenek például:

- A szokásosnál tovább töltődnek be a programok,
- furcsa hibaüzenetek jelennek meg,
- lecsökken a memóriatartomány, a szabad tárterület,
- a winchester sokáig, látszólag céltalanul működik (miközben nem futtatunk külön programot),
- eltűnnek fájlok,
- gyakoriabbak lesznek a lefagyások,
- programállományok hossza látszólag ok nélküli megváltozik.

Hogyan védekezhetünk a vírusok ellen?

- A legegyszerűbb védelem: ne tegyünk be idegen lemezt a gépbe, ne indítsunk (bootoljunk) idegen lemezről, és ne másoljunk át a winchesterünkre bizonytalan eredetű programokat azok előzetes ellenőrzése nélkül!
- Csak jogtiszta szoftvereket használjunk, mert az illegálisan másolt programok fertőzésveszélyt hordoznak!
- Adatainkról rendszeresen készítsünk biztonsági másolatot!
- Ha nyilvános hálózati kapcsolattal rendelkezünk, gondoskodjunk megfelelő biztonságot nyújtó tűzfal kiépítéséről. A tűzfal lényegében a hálózat és a számítógép közötti szoftveres védelmi rendszer. A tűzfal korlátozhatja, hogy milyen adatok kerüljenek a számítógépünkről a hálózatra és fordítva.
- Csak olyan e-maileket nyissunk meg, amelyek ismert helyről érkeznek és értelmes, a feladóval összefüggésbe hozható a tárgyuk.
- Figyeljünk rá, hogy a csatolmányunknak milyen kiterjesztése van. A vírusok megpróbálják álcázni magukat.

Milyen fajtái vannak a vírusoknak?

- Bootvírusok

A boot vírusok az elsőként megjelenő vírusok közé tartoznak. Leggyakrabban akkor terjednek, ha fertőzött lemezzel indítjuk el a rendszert. Ebben az esetben a vírus a merevlemez boot szektorába ágyazódik be, így még az operációs rendszer betöltése előtt aktiválódik. Ennek hatására a fertőzött merevlemez az összes meghajtóba helyezett lemezt megfertőzi. A boot vírusok napjainkban a kevésbé elterjedt vírusfajták közé tartoznak.

- Alkalmazásvírusok

Az alkalmazás- vagy más néven programvírusok a futtatható kódot tartalmazó (.COM, .EXE kiterjesztésű) állományokat fertőzik meg. A megfertőzött állományokba beírják a saját kódjukat.Két fajtáját különböztetjük meg: hozzáfűződő (append) és felülíró (replace) vírusokat. A hozzáfűződő vírusok az alkalmazások végéhez fűződnek, elhelyeznek azonban a program elején egy kódot, hogy az alkalmazás indulásakor előbb ők töltődjenek be, a program csak később. A felülíró vírusok az alkalmazások elejét írják felül saját kódjukkal, így a fertőzött állomány adatot veszít, és az eredeti állapot nem

állítható helyre. Amennyiben egy programvírussal fertőzött fájlt elindítunk, a vírus betöltődik a memóriába és megfertőzi az összes többi elindított programot.

- Makrovírusok

Elsősorban olyan dokumentumszerkesztő programokat támadnak meg a makrovírusok, melyek elég fejlettek, hogy bizonyos lépéssorozatokat képesek legyenek makrókkal automatizálni. Általában Word és Excel által készített dokumentumokat (.DOC, .XLS) fertőznek meg. Terjedésükhöz elegendő egy fertőzött állomány megnyitása, és a vírus már be is töltődik a memóriába, mely a későbbiekben megnyitott dokumentumokat megfertőzi. A fertőzést általában már csak akkor vesszük észre, amikor már késő.

A makrovírusok csoportjába tartoznak a levelező vírusok is, melyek elsősorban e-mail útján terjednek. A csatolt fertőzött fájlok megnyitásakor aktivizálják magukat és általában a levelezési listában szereplő partnereknek írnak levelet, melyhez saját maguk másolatát is hozzáfűzik. Ha a levelezési címlistában nagyon sok partner van, akkor olyan mennyiségű levéláradat indulhat, amely megbénítja egy nagyvállalat levelezőrendszerét is.

- Férgek

Terjedésük szempontjából a féreg vírusok eltérő viselkedésűek, mivel nem hagyományos értelemben fejtik ki károkozó hatásukat, hiszen nem tesznek kárt állományainkban. Elsősorban interneten, hálózaton terjednek. Megbújnak a számítógépen, és információt gyűjtenek róla, majd az összegyűjtött információkat tárolják. Ha ismét csatlakozunk az internetre, hálózatra, akkor ezeket a tárolt információkat a megadott címre továbbítják.

- Spyware

A spyware vagy más néven kémprogramok célja, hogy adatokat gyűjtsenek személyekről vagy szervezetekről azok tudta nélkül a számítógép-hálózatokon. Az információszerzés célja lehet például reklámanyagok eljuttatása a kikémlelt címekre, de akár ellophatják jelszavainkat, számlaszámainkat vagy más személyes adatainkat rosszindulatú akciók céljából is. A vírusokhoz hasonlóan lehet őket „beszerezni”.

Mi a feladata a vírus kereső, - mentesítő programoknak?

A víruskereső-, figyelő- és irtóprogramoknak az a feladata, hogy

- Megakadályozzák a vírusok bejutását a gépünkbe.
- Ha már bejutott a vírus, akkor felismerjék, és lehetőleg eltávolítsák.
- Megakadályozzák, hogy a számítógép továbbadja a fertőzést.

Milyen szolgáltatásai vannak a víruskereső programoknak?

- A helyi és csatolt meghajtók időzíthető ellenőrzése. A programot be lehet állítani, hogy bizonyos időszakonként ellenőrizze a merevlemezen, optikai meghajtón, hálózati meghajtón tárolt valamennyi állományt. Ez a „teljes rendszerellenőrzés” nem csak automatikusan időzítve, hanem a felhasználó kérésére is elindítható.
- Programok, dokumentumok ellenőrzése a megnyitásuk, letöltésük pillanatában.
- A vírusinformációk rendszeres frissítése.
- Az állományokat ellenőrző kódokkal látja el, amelyek az állomány megváltozása esetén azonnal gyanús tevékenységre lehet következtetni.

Milyen vírusirtó programokat ismersz?

AVG Panda Norton Nod32 AVAST McAfee

02/10. GYAKORLATI FELADAT

1.) Keresd meg a számítógépeden lévő vírusirtó programot! Indítsd el az alkalmazást!
2.) Nézd meg (keresd meg), hogy mikor lett frissítve a program vírus adatbázisa!
3.) Futtass egy teljes ellenőrzést a C: meghajtón!
4.) A jelentést mentsd txt formátumban az asztalra!