

Tartalomvédelem: DRM

oktatási segédanyag az „IP alapú távközlés” c. tárgyhoz

Készült:

Bedő Balázs

Digitális szerzőijog-védelem

című szakdolgozatának felhasználásával.

Szerkesztette: Lencse Gábor

Az anyag témaköre:

Tartalomvédelem: DRM

A szakdolgozat a következő részeket foglalta magában:

- Tekintse át, milyen megoldások vannak digitális szerzőijog-védelemre!
- Elemezze a megoldásokat szakmai (kijátszhatóság) és társadalmi szempontból! Mutasson be gyakorlatban is néhány megoldást a jogtalan felhasználásra!
- Tervezzon egy egyszerű, mobiltelefon készüléken is használható megoldást. Implementálja és mutassa be működését. Elemezze biztonsági szempontból! (ezt az anyagból kihagytam!)
- Mutassa be személyes jövőképét a digitális szerzőijog-védelemről!

Tartalomjegyzék

1. Bevezető.....	1
2. A szerzőijog-védelemhez vezető út.....	3
3. A DRM rendszerek bemutatása.....	6
3.1. A szoftverpiac.....	6
3.2. Az audió CD.....	8
3.3. A DVD.....	11
3.4. A nyomtatott sajtó.....	14
3.5. A mintavételezett audió tartalmak.....	15
3.5.1. Apple FairPlay DRM.....	15
3.5.2 Windows Media DRM.....	18
3.6. Blu-ray Disc és HD DVD.....	21
3.7. A felhasználói élmény.....	26
3.8. Összefoglalás.....	31
5. A DRM jövője.....	32
5.1. Szigorú konzervatív.....	33
5.1.1. Erősebb kontroll.....	33
5.1.2. Új jogszabályok.....	34
5.2. Megengedő innovatív.....	35
5.2.1. Új jogi hozzáállás.....	35
5.2.2. Új üzleti modell.....	36
6. Összefoglalás.....	41
7. Irodalomjegyzék.....	43

1. Bevezető

A digitális technológia térhódításával gyakorlatilag megszűntek a másolatkészítés költséges anyagi korlátai. Hiszen az analóg időkben minden másolathoz szükség volt az adott médiatípushoz szükséges technikai háttére, valamint a megfelelő, nyers adathordozóra. Ebben a korszakban a másolás kötelező velejárója volt a minőségromlás is, ami különösen a másolatok másolatainak elkészítésekor okozott problémát. Szintén nehezítette a "kalózok" dolgát, hogy lemásolni csak egy valóságosan birtokolt adathordozót lehetett.

A digitális technológiának köszönhetően egyetlen, szinte mindenki számára rendelkezésre álló eszközzel, a számítógéppel, az eredetivel tökéletesen egyező másolatot lehet készíteni szinte bármilyen digitálisan tárolt tartalomról. Nem csoda tehát, hogy a tartalomszolgáltatók igyekeznek megakadályozni ezt a fajta cselekedetet.

A legsúlyosabb problémát azonban az internet villámgyors térnyerése okozta. A világháló segítségével úgy lehet az eredetivel tökéletesen megegyező kópiát készíteni egy digitális tartalomról, hogy a forrás akár egy másik országban is lehet.

Így nincs könnyű helyzetben senki, aki a digitális másolatkészítés megakadályozására törekszik. Az informatika megjelenésével és robbanásszerű elterjedésével a legtöbb iparág kénytelen volt nyitni az új technológia felé, és az addig kizárólag fizikailag létező termékeiket digitális formában is a vásárlók részére bocsájtották. A másolás megakadályozása azonban nem könnyű, sőt megkockáztatom kijelenteni, lehetetlen feladat egy olyan közegben ahol minden az adatok másolásán alapszik. A Neumann János által kidolgozott számítógép architektúrájában is kitűnik, az adatok folyamatos másolása zajlik a memória, a processzor, és az aritmetikai és logikai egység között.

Számos megoldás született a problémára, azonban valódi célját csak nagyon kevés érte el. A *megoldások gyakran társadalmi és technológiai problémákat okoztak*, és az emberek megítélése rendkívül rossz ezekről. Gyakran előfordul, hogy a DRM rendszerek a tartalomnak azon tulajdonságát korlátozzák, mely korábban analóg adathordozón tárolva magától értetődő volt. Ilyen tulajdonság például a *kölcsönadhatóság*, valamint a *továbbértékesítés*.

Az esetek túlnyomó többségében a megoldások megakadályozzák a *biztonsági másolatok elkészítését* is. Tovább súlyosbítja a helyzetet, hogy a *jogalkotók elfogadták ezeket a*

korlátozásokat és szárnyaik alá vették ezeket a rendszereket.

A jogi szabályozás, a technológia ismerete és birtoklása, valamint a másolatkészítés költsége van közvetlen hatással egy termék másolásának bekövetkezésére. Azon iparágak szereplői, melyek a szellemi tulajdonra épülnek, erre a négy tényezőre igyekeznek hatást gyakorolni. A termékek másolásának alapja természetesen a kereslet, mely az egész rendszert mozgásban tartja.

A digitális technológia elterjedéséig a termékek tulajdonosai, általában a kiadók jogi megoldásokkal igyekeztek megvédeni tulajdonukat. Majd az új rendszerek megjelenésével egy időben kezdtek mind a négy tényezőre nyomást gyakorolni.

A rohamléptekkel fejlődő informatika vívmányainak képtelenek voltak gátat szabni ezekkel a módszerekkel. Sorra születtek olyan megoldások, melyek valamilyen termékhez kötötték a tartalmat, vagy valamely más módon korlátozták a szabad felhasználást.

Az on-line tartalomszolgáltatók, zeneáruházak mindegyike megpróbálkozott valamilyen DRM rendszer alkalmazásával, mindegyik különbözővel. Talán ennek is köszönhető volt, hogy mára az összes piacvezető zeneáruház DRM nélkül, teljesen védtelenül, szabadon másolhatóan is forgalomba hozza a felvételeket.

Dolgozatomban végigjárom, hogy milyen út vezetett a digitális tartalomvédelemig, jellemzem a megoldásnak szánt technológiákat és azok hibáit, társadalmi és jogi megítélését, valamint bemutatok egy általam tervezett rendszert.

2. A szerzőijog-védelemhez vezető út

„A könyvek, zenék, filmek a közjavak két tulajdonságával is rendelkeznek. Korlátlan mennyiségben fogyaszthatók anélkül, hogy elfogynának és nem-kizárólagosak, azaz nehéz megtiltani, hogy hozzáférjenek. Ez a két tulajdonság az, ami miatt a kreatív tevékenység kevés hasznot hozhat egy művész számára, mivel alkotásához bárki, bármennyiszer hozzáférhet anélkül, hogy kompenzálnia kéne a művészt. A jelenség korlátozására, és a kreatív alkotások támogatására jöttek létre a szerzői jogi szabályok, amelyek az alkotók számára meghatározott időre kizárólagosságot biztosítanak műveik felett, beleértve annak másolását és terjesztését.” (Paul Petrick - 1995)

A szerzői jog a nyomtatott könyvek megjelenésével egyidős. Célja biztosítani a könnyen másolható termékek védelmét. „Eleinte eseti alapon történt a jogok odaítélése. Kizárólagosság jogát első esetben a Velencei köztársaságban ítélték oda egy könyv kiadójának 1486-ban, bár egyes jelek arra utalnak, hogy az ókori Görögországban már volt hasonló szabályozás. Franciaországban 1503-ban, Angliában 1518-ban biztosítottak kizárólagos jogot először, ez utóbbi országban a Királyi Nyomda számára. A kizárólagosság változó időtartamra vonatkozott. A Velencei köztársaság esetében ritkán haladta meg a 14 évet, míg Angliában pár évre szólt csak. A jogi védelem igénye elsősorban a kiadóktól származott. A szerzői jog modern koncepciója, mely a szerzőket helyezi előtérbe, Angliából származik. Az 1710-ben alkotott szabályozás biztosított először korlátozott időtartamra kizárólagos jogokat a szerzőnek – és nem a kiadónak.” (Wikipedia – History of copyright law)

Az 1920-as évektől megjelentek az otthonokban a rádiókészülékek és a rádiószolgáltatás, mely az érdeklődők számára „másolta” a zenét. Mindezt úgy tették, hogy egy új példány létrehozása, azaz egy hallgató bekapcsolódása nem járt plusz költséggel a rádióadó számára. 1938-ra Amerikában a háztartások 80%-ában volt rádiókészülék. Ebben az évben a korábbi 75 millió dollárról a zeneipar bevétele 26 millió dollárra csökkent. Ezután a rádiótársaságoktól a kiadók jogdíjat kezdtek szedni. (Wikipedia – History of radio)

A rádiók valójában nem voltak a hanglemezek konkurenciái, hisz ahhoz, hogy valaki bármikor, bármennyiszer meghallgathasson egy felvételt kénytelen volt megvásárolni az eredeti terméket.

Ugyanez elmondható a televízió készülékek megjelenéséről is, hisz egyik esetben sem volt mód a rádió, vagy tévéadás rögzítésére.

A rögzítőeszközök megjelenése a zeneipar és a filmipar számára is ijesztő pillanat volt. Ez volt az a pont, amikor a technológia a másolás lehetőségét a lakosság kezébe adta, és lehetővé tette másolatok egyszerű készítését bizonyos korlátozásokkal. A származékos példány még nem volt tökéletes másolata az eredetinek, néhány iteráció után a minőség rendkívül leromlott. Bár az azóta eltelt idő megmutatta, hogy a hangkazetta és a videokazetta óriási piacot hozott létre az ipar számára, mégis 1983-ban Jack Valenti, az MPAA elnöke a következőt nyilatkozta a videórögzítőkről: "Egyesek szerint a VCR az amerikai film producerek legjobb barátja. Én azt mondom nektek, hogy a VCR olyan az amerikai film producereknek és Amerika népének, mint a Bostoni fojtogató egy magányos nő számára."

A rögzítőeszközökkel szembeni hadjárat eredménye az lett, hogy a magáncélú rögzítéseket a bíróság szabad felhasználásnak minősítette, és emellett az is elfogadásra került, hogy ha egy eszköz használható jogsértő célra, valamint nem jogsértő célra is, úgy az eszköz maga nem tekinthető jogsértőnek. [34]

A kazettás magnó és a videófelvevők viszonylag olcsó eszközzé váltak, és a másolatok készítéséhez használt mágnesszalagos tárolók sem voltak drágák, így kellően el tudtak terjedni. Az ipar és a kormány az „üreskazetta” jogdíjjal reagált, melynek összege beépült az eszközök és tárolók árába. Az eszközökre kivetett jogdíjak megemelték a másolási eljárások költségének fix és változó részét, ám nem jelentős mértékben. A jogi szabályozáson az eszközök megjelenése közvetlenül nem változtatott. Közvetett hatása azonban lehetett abban, hogy a 80-as évektől a szerzői jog által biztosított kizárólagosság időtartama egyre hosszabbra és hosszabbra nyúlt.

A filmipar nem törődött bele a vereségbe, és a történelemben először itt alkalmaztak másolásvédelmet. A műsoros videokazettákat körülbelül 1985-től egy macrovision nevű másolásvédelmi megoldással hozták forgalomba. A rendszer lényege, hogy a függőleges szinkronjel után, a feketeszint idején nagyszintű tüskéket tettek a videójelre. Ettől aztán a videóknak szétesett a szinkronizálása, aminek eredménye az élvezhetetlen, színtelen kép lett.

Leleményes felhasználók felfigyeltek rá, hogy a másolásvédelem nem minden videómagnóra van hatással. Különösen igaz volt ez a régebbi típusokra. Később kiderült, hogy egy szerzői jogi határozat értelmében a videómagnó gyártóknak kötelező volt olyan komponenst építeni

készülékeikbe, amik érzékenyek voltak a zavaró jelekre. Nem telt bele sok idő, megfejtették a másolásvédelem módszerét és elkészítették a dekódert, mely kiszűrte a zavarójelet. Egy 1988-ban megjelent német elektronikai folyóiratban teljes kapcsolási rajz, alkatrészlista és elkészítési utasítás állt rendelkezésre. Magyarországon 1995-ben, amikor még javában zajlott a videókazetta másolás, egy ilyen szerkezet előállítási költsége körülbelül 1500 forint volt.

Tulajdonképpen azonban ez a megoldás elérte célját. Az átlagfelhasználó képtelen volt lemásolni a védett tartalmat.

3. A DRM rendszerek bemutatása

A digitális jogkezelés (Digital Rights Management - DRM) fogalma: a digitális tartalmakhoz való hozzáférést lehetővé tevő, illetve szabályozó technikai, műszaki, hardver- és szoftvereszközök összefoglaló neve.

A DRM a digitális tartalom szabályozására és ellenőrzésére különböző technikákat alkalmaz, különösképpen rejtjelezést, megjelölést, vagy szelektív inkompatibilitást:

- **Rejtjelezés** (Encryption): A rejtjelezett információkhoz a felhasználó csak a rejtjelező kulcs birtokában férhet hozzá. Ez a kulcs gyakran a tartalomhoz való hozzáféréshez használt hardveren vagy szoftverben található. Erre példa a DVD-lejátszó: A lejátszó készülék tartalmazza a DVD-k lejátszásához szükséges kulcsot.
- **Megjelölés** (Marking): Az adatokat a jogtulajdonos az értékesítés előtt megjelöli a tartalomról szóló információk továbbvitele érdekében. Ilyen információ például, hogy az adat másolásvédelem alatt áll, vagy ki a jogtulajdonos, illetve milyen felhasználási módok megengedettek (DVD átugorhatatlan részek).
- **Szelektív inkompatibilitás** (Selective Incompatibility): Amikor a gyártó például hibákat kódol egy CD tartalmába annak érdekében, hogy a hanghordozót számítógéppel, autórádióval, hordozható lejátszó készülékkel, mobiltelefonnal, stb. ne lehessen lejátszani.

A következő fejezetekben bemutatom a digitális szerzőijog-védelem által leginkább érintett területeket, a létező megoldásokat, azok hibáit, illetve ezen hibák kihasználásának módjait.

3.1. A szoftverpiac

A DRM rendszerekre már akkor megjelent az igény, amikor a számítógép ipar a szabványosítás útjára lépett, és egy szoftver előállításával nemcsak minimális méretű piacot lehetett elérni, hanem jelentősen kitágult potenciális felhasználói bázist is. Az igényt erősítette még a hardver- és szoftver-értékesítés elválása. Míg a hardver komponenseket továbbra is meg kellett venni, addig a hozzájuk tartozó szoftvereket elég volt kölcsönkérni egy másolás erejéig.

A szoftverek esetében az alacsonynak tartott eladások miatt került a digitális jogkezelés a vállalatok fókuszába. Az előállított szoftverek jelentős részét másolták, köztük olyan felhasználók is, akik a másolt szoftvert használva szereztek bevételeket. Az ezzel kapcsolatos aggályok nagyon hamar megjelentek. 1976. február 3-án Bill Gates nyílt levelet intézett azon hobbistáknak, akik másolt szoftverekkel használták számítógépüket.

Bill Gates a levélben leírja, hogy az Altair BASIC (Az Altair BASIC a „Micro-Soft” első terméke volt) programba fektetett munkája, ideje és az abból befolyt jogdíjak alapján 2 dolláros órabér számolható ki neki. Ugyanitt megjegyzi, hogy a szoftver kalózkodás az oka annak, hogy nem születnek jó alkalmazások.

„Egy dogot azonban sikerül elérnetek, megakadályozzátok, hogy jó szoftverek íródjanak. Ki engedhet meg magának professzionális munkát a semmiért? Melyik hobbista lenne képes 3 évnyi munkát fektetni a terméke programozásba, hibakeresésbe és dokumentálásába, majd ingyen szétosztani?”

Bill Gates – 1976. február

Ennek ellenére 1970 óta a Microsoft az egyik legnagyobb IT vállalkozássá nőtte ki magát, és a 2007 januárjában futótűzként terjedt hír szerint a Microsoft termékek 22%-a vélhetően illegális példány.

Bár ez meglehetősen alacsony értéknek tűnik. A IDC által készített BSA tanulmány szerint 2005-ben a világ szoftvereinek 35%-a volt illegális másolat, mely 35 milliárd dollár veszteséget okozott a szoftverkészítő vállalatok számára. Ebből az összegből 6,9 milliárd dollár veszteséget az amerikai, 3,9 milliárd dollár veszteséget a kínai és 3,2 milliárd dollár veszteséget a francia szoftver ipar szenvedett el. Becsléseik szerint a kalóz másolatok arányának 10 százalékpontos csökkentése 2,4 millió új munkahelyet teremtené, valamint 400 milliárd dolláros gazdasági növekedést, és 67 milliárd dolláros éves adóbevétel-növekedést okozna. [9]

A Microsoft oldalán elérhető tanulmány szerint 2007-ben a világon használt szoftverek 55%-a kalóz verzió. Közép- és Kelet-Európában ez az arány 69%-os (BSA [2007]), dacára a különféle másolás ellenes törekvéseknek. A BSA magyarországi honlapján található adatok szerint Magyarországon a szoftverek 42%-a illegális forrásból származik, és a szoftverkalózkodás 22 milliárd forint veszteséget okoz évente a szoftver ipar számára. Az IDC 2005-ös és 2006-os tanulmányaira hivatkozva BSA azt állítja, a kalózmásolatok

arányának 10 százalékpontos csökkentése 155 milliárd forint bevételt termelne az ország számára, és további 31 milliárd forint adóbevétellel járna. [9]

LG megjegyzései:

1. A fenti számítások formálisan ugyan megtehetőek, de nélkülözik a gazdasági realitást: például a tinédzserek többségének NINCS annyi pénze, hogy megvegye az általa használt lopott szoftvereket. Az illegális szoftverhasználat alternatívája NAGYON SOK ESETBEN nem a megvásárlás, hanem a szoftver használatától való tartózkodás, ami mellesleg sokszor kifejezetten JÁRHATÓ ÚT! (A legtöbb esetben a valóban fontos célokra léteznek *ingyenes* vagy akár *szabad szoftverek* is...)
2. Valamikor 1985 és 89 között (középiskolában) mondta egyik tanárom, hogy az USA-ban egy szövegszerkesztő ára körülbelül egy férfiing árának felel meg. Magyarországon az ár arányok ma is kb. tízszeresek, ha pl. a Microsoft Office-ra gondolunk. Így az illegális szoftverhasználat nálunk ma nem pusztán erkölcsi, hanem erősen anyagi kérdés is.
3. Mielőtt valaki gyűjtést szervezne Bill Gates megsegítésére, tudnia kell, hogy ő az USA egyik leggazdagabb embere. Mellesleg sokan fejlesztenek szoftvert ellenszolgáltatás nélkül GPL licenc alatt, és ezek egy része (pl. Debian GNU/Linux) sokkal stabilabb, megbízhatóbb, a szabványokat kevésbé megsértő, logikusabb félépítésű/működésű stb., mint a szóban forgó szoftver cég programjai.
4. **A fentiek természetesen senkit sem jogosítanak fel illegális szoftverhasználatra!** (Csupán a helyzetet árnyalására írtam ide.)

A játékszoftver ipar számára a helyzet némileg eltér az előbb tárgyalt vállalatokétól. A játékszoftverek célpiaca a lakossági, azon belül is a fiatalabb korosztály, mely inkább hajlik az illegális másolatok beszerzésére, különösen ha önálló jövedelemmel nem rendelkezik. A vállalatok könnyebben ellenőrizhetőek, mint a lakosság, részben számosságuk, részben felkutathatóságuk miatt, így a játék ipar számára kiemelten fontos volt mindig is, hogy a felhasználókat legálisan megszerzett példányok futtatására kényszerítse. Mivel ez a szegmens fedi le leginkább a számítógéphez értő hobbisták körét, így a számítógépes játékok kalózzai rendelkeznek a legnagyobb humán kapacitással a legalitást vizsgáló algoritmusok feltörése érdekében.

2004-ben a játékipar bevétele az Egyesült Államokban 7,3 milliárd dollárt tett ki. Becslések szerint a kalózmásolatok miatt ugyanitt az ipart 1,8 milliárd dollár veszteség érte. A kalózkodás negatív hatásaival azonban nem csak a játékkészítők szembesülnek. Előfordulnak a folyamatnak olyan nehezen azonosítható kárvallottjai is, mint a hardver gyártók. Példaként megemlíthető a Half-Life 2 nevű játék forráskódjának 2003-as kiszivárgása. Az adatok szerint az incidens jelentős problémákat okozott az ATI-nak azáltal, hogy a játék tényleges kiadását a

kiszivárgás miatt hónapokkal eltolták, felrúgva ezzel az ATI előzetes üzleti terveit.

A történet annyiból ironikus, hogy a videokártya-gyártók a játékszoftver kalózkodás első számú élvezői, hiszen a számtalan, egyre nagyobb teljesítményt igénylő játékok miatt vásárolják az egyre újabb videokártyákat is.

3.2. Az audió CD

A zeneipar az előbb említett játékiparral ellentétben jóval később reagált a kalózkodásra. Habár első termékük, a bakelit lemez még nem volt másolható otthoni készülékekkel, a mágneskazettát már könnyen lehetett sokszorosítani egy-két alkalommal, amíg a plusz kópia hangminősége az élvezhető szint alá nem csökkent. Az magnókazetták okozta problémát az ipar és az állami szervek az „üreskazetta díj” bevezetésével oldották fel, mely minden üres adathordozó után egy meghatározott összegre jogosította fel a közös jogkezelő szervek kezelésén keresztül az ipar szereplőit. *Magyarországon a közös jogkezelőkhöz befolyt összeg szétosztásának módját törvény szabályozza.*

A CD lemezek 1982-83-as megjelenése ellenére az igazán komoly kalózkodás és fájlcsere ellenes kampányt csupán 1998-ban kezdte el az Amerikai Zeneipari Szövetség (RIAA), amikor Hilary Rose került a szervezet élére. A RIAA becslései szerint az illegális példányok miatt a teljes ipart évi 4,2 milliárd dollár veszteség éri évente. [33]

A globális CD eladások száma 2000-től 2006-ig 23%-al csökkent. A Big Champagne Online Media Measurement szerint havonta 1 milliárd digitális zene másolatot cserélnek a felhasználók, míg az Amerikában 70%-os részesedéssel rendelkező iTunes Music Store 2003 és 2007 között körülbelül 2 milliárd zeneszámot értékesített összesen.

Ellenlépésként olyan CD-k kerültek piacra, melyeket a számítógépek CD-ROM olvasói nem tudtak kezelni, csak az újabb asztali lejátszó berendezések, így akadályozva meg a CD-k tartalmának könnyen terjeszthető formátumba való számítógépes konvertálását. Az első kiadó, amely DRM-el látta el az audió CD termékeit a BMG volt 2002-ben. [24]

A különféle digitális jogkezelő rendszerek ezután egyre elterjedtebbé váltak, míg a Sony „rootkit” botránya 2005-ben fel nem hívta a közönség figyelmét a benne rejlő veszélyekre.

2005. október 31-én egy Microsoft alkalmazott teljesen véletlenül észrevette, hogy a

számítógépe rootkit-el fertőződött meg. *A rootkit technológia lényege, hogy eltüntet alkalmazásokat és alkalmazásokhoz tartozó beállítások minden jelét a felhasználó szeme elől úgy, hogy azok a valóságban továbbra is a számítógépén maradnak.* Míg egy vírus, trójai vagy féreg futtatható állománya, és működésének nyomai megtalálhatók egy fertőzött rendszeren, addig egy rootkit technológiával felvértezett szoftver a felhasználó számára láthatatlan.

Miután Mark Russinovich egy véletlen folytán észrevette, hogy számítógépe rootkit szoftvert futtat, sikeresen eljutott a szoftver gyökereihez, és kiderítette, hogy az a nemrégiben megvásárolt zenei CD-jéről másolódott fel számítógépére a tudta nélkül. Az együttes kiadója a Sony volt. A CD végfelhasználói licencszerződésben egyetlen szó sem esett arról, hogy rootkit szoftver fog települni a számítógépre. A szoftver folyamatosan figyelte a számítógép fájljait, és az optikai meghajtókon történő műveleteket. A rootkit technológia pedig minden olyan fájlt, beállítást láthatatlanná tett, aminek a nevében a „\$sys\$” karaktersor szerepelt. A szoftver az elkendőzést nem csak a saját fájljain hajtotta végre, hanem bármilyen fájlra, ami a merevlemezen megfelelő névvel található volt. Egy olyan számítógépes bűnöző, aki ártó szándékú programjának nevébe ezt a karaktersort helyezte, el tudta érni, hogy felhasználó gépén titokban futó Sony rootkit program a bűnöző kártékony programjának jelenlétét is láthatatlanná tegye. Mark Russinovich felfedezése a blogszférában rendkívül felkapott témává vált, és november 3-án a Sony közzétett egy javítást, amely a már bevallottan másolásvédelmi feladatokat ellátó szoftvernek kikapcsolja a rootkit tulajdonságát, azaz láthatóvá tesz mindent, amit addig eltitkolt. A javításhoz csak interneten keresztül lehetett hozzáférni, és minden fertőzöttnek az email címével kellett jelentkezni a Sony honlapján. Azok a vásárlók, akik nem rendelkeztek internettel, valójában nem is juthattak hozzá a javításhoz. Russinovich arra is rájött, hogy a DRM rendszer a lejátszott CD-k azonosítóját rendszeresen elküldi a Sony-hoz, bár a licencszerződést ezt nem említette, és később a Sony vezetők tagadták.

Egyes elterjedtebb CD/DVD másoló programok olyan funkcióval jelentek meg, amelyek védettek voltak a Sony rootkit DRM-jével szemben.

Azonban a Sony CD-lemezein alkalmazott XCP DRM-et nem tudták feltörni, ám ennek használata olyan botrányhoz vezetett, hogy végül maga a Sony döntött úgy, hogy felhagy alkalmazásával.

Fred von Lohmann, az EFF jogásza a Sony végfelhasználó licencszerződését

áttanulmányozta, s számos szokatlan korlátozást talált benne. Ezután az EFF olyan felhasználók után kezdett kutatni, akik megvásárolták az ominózus CD-t, hogy közösen pert indíthassanak a Sony ellen. Később a Sony képviselője kijelentette, hogy a kiadó többé nem terjeszt rootkittel ellátott zenei CD-ket.

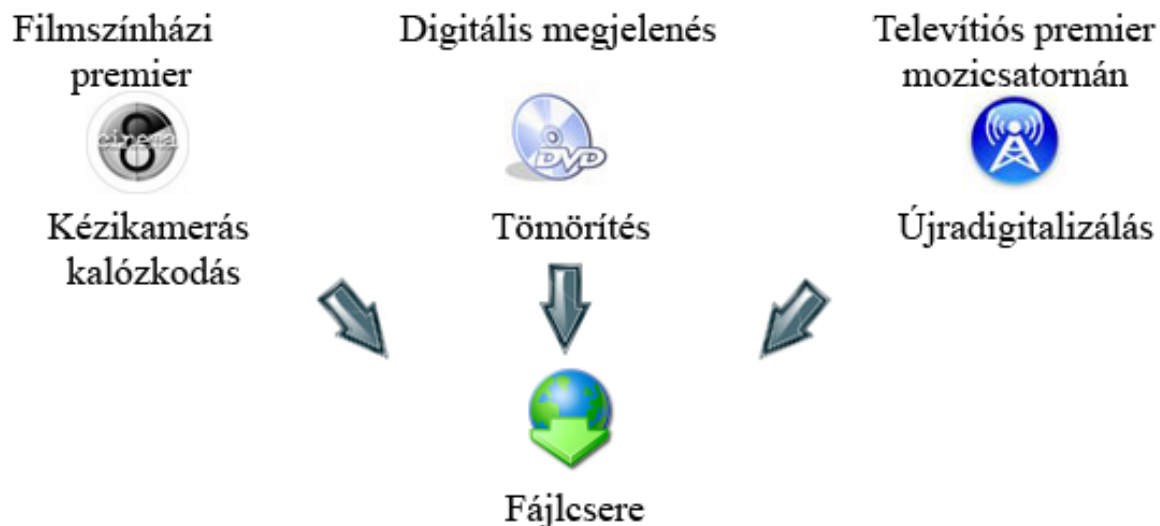
Egy másik blogger, Alex Halderman más Sony CD-ken is talált addig ismeretlen másolásvédelmi szoftvereket, amik szintén adatokat közöltek a felhasználóról a Sony számára.

Egy finn kutató azt is leírta, hogy a Sony javítása számtalan hibát hagy hátra a felhasználó számítógépén, és ezt bizonyítandó készített egy olyan weboldalt, amelynek pusztán meglátogatása is képes újraindítani a „javított” számítógépet. Továbbá az is kiderült, hogy *a Sony DRM rendszere egy nyílt forráskódú szoftverből kölcsönzött kódrészleteket, s mivel a Sony a licencfeltételeknek nem felelt meg, így jogsértést követett el.*

A Sony ellen indított perek megállapodással zárultak. Az áldozatok kártérítésre tarthatnak igényt, amelyet vagy pénzben vagy szolgáltatásban törleszt a vállalat.

3.3. A DVD

A filmipar is hasonló jelenséggel szembesült, mint a zeneipar. A filmipar helyzete azonban egyszerre érzékenyebb, és biztosabb a zeneiparénál. A zenei termékek piacra kerülése egylépcsős folyamat: a CD-k megjelennek a boltokban. A filmek esetében az eladható tartalom több különböző formában és eltérő időpontokban jelenik meg a piacon, és emiatt több ponton is támadhatóak a kalózok részéről. A zeneiparhoz képest mégis több lábon állnak, és jóval több embert érnek el.



1. ábra A filmek megjelenésének fázisai

A film először a filmszínházakban kerül bemutatásra. A bemutatót követően gyakran kézikamerával felvételt készítenek a vászonról, és az internet segítségével meg is osztják ezt a felvételt. Ennek a módszernek nincs különösebb veszélye, mivel az ilyen módon készült felvétel rendkívül rossz minőségű, élvezhetetlen.

A folyamat következő lépése: a film DVD-lemezen kerül a kölcsönzőkbe, illetve a boltok polcaira. Ez az a pont, amitől kezdve egy film teljes egészében hozzáférhető digitális formában, rendkívül jó minőségben.

A tartalom DRM szempontjából érdekes életének utolsó fázisa, a mozicsatornákon történő bemutatás. Ebben a stádiumban általában analóg formában kerül a felhasználóhoz a film, a sorozat. Gyakran előfordul, hogy számítógéppel felvételt készítenek a műsorról, majd azt az internet segítségével teszik „közkinccsé”. Ezzel a 3.7. fejezetben foglalkozom.

A DVD-lemezek védelmére 1996-ban vezették be a **Content Scramble System (CSS)** DRM sémát amit a *tartalom titkosítására, a kalózmásolatok elkészítésének megakadályozására fejlesztettek ki, valamint ez biztosítja a régiókódok működőképességét, a DVD indítása utáni figyelmeztető részek átugorhatatlanságát, illetve más korlátozásokat.*

A CSS algoritmus eredetileg titkos volt és architektúrális zártság jellemezte. A titkosításhoz 40 bites kulcsokat alkalmaztak. Ez az akkori amerikai szabályozásnak, illetve annak a koncepciónak alapján tűnt elégségesnek, hogy eredetileg mindenki a Matsushita nevű szállítótól vásárolta volna a titkosításért felelős egységet.

A CSS rendszerben használt kulcsok:

- Hitelesítési kulcs (KA): a kölcsönös hitelesítés folyamán alkalmazott titok
- Viszony (busz) kulcs (KSES): a hitelesítés folyamán jön létre, a fejléc- és lemez kulcsok titkosítására
- Lejátszó kulcs (KP): a DVD lejátszót gyártó cég egyedi kulcsa (DVD CCA). DKP (KD)
- Lemez kulcs (KD): EKD (KT)
- Szektor kulcs (KSEC): minden szektorhoz tartozik egy 128 bájtos nyílt szövegű fejléc.

Ezen fejléc 80-84. bájtja a szektor kulcs.

- Fejléc (title) kulcs (KT): $E(KT+KSEC)$, szektor adat)

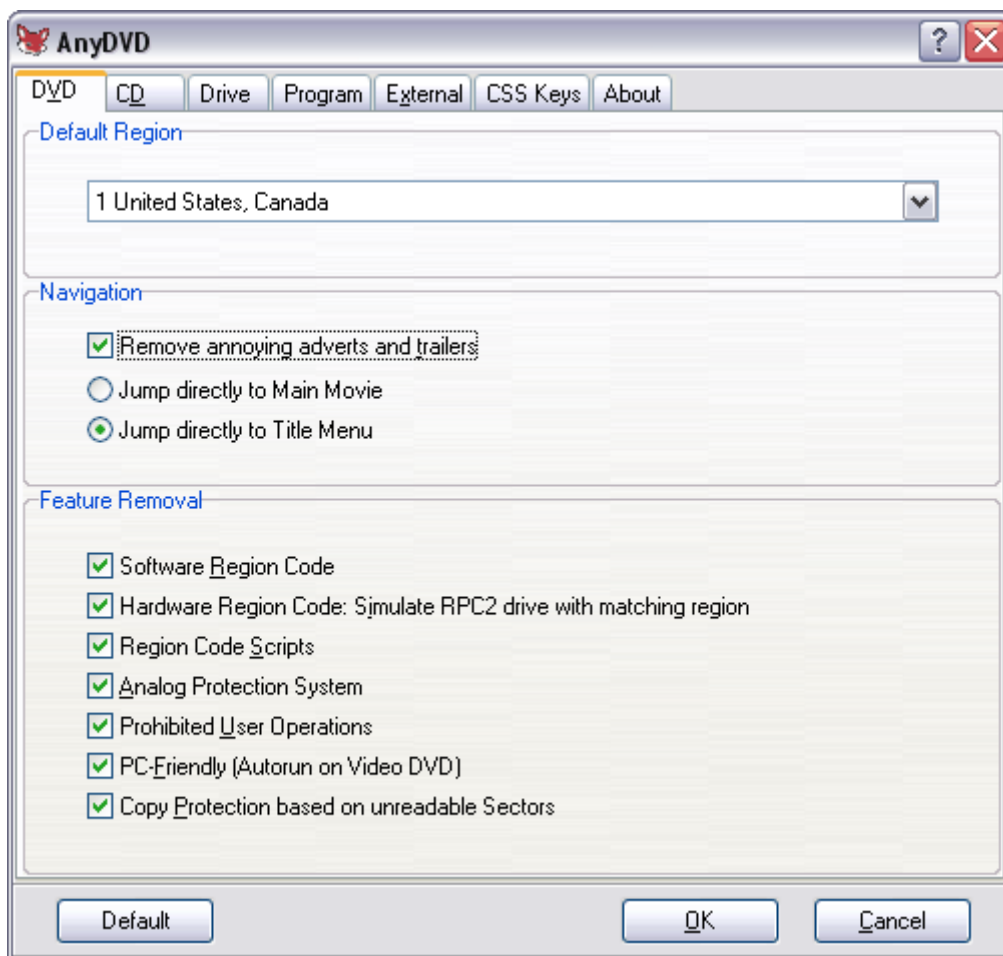
Tehát minden lejátszóban található a gyártójához tartozó lejátszó kulcs. Ezzel lehet kikódolni a lemez kulcsot. A lemezen a következő információkat tárolják:

- hash (KD): 5 bájtos
- Lemez kulcs az egyes lejátszók kulcsaival: $KD1 = EKP1(KD)$, $KD2 = EKP2(KD)$, ...

A CSS-ben alkalmazott folyamkódoló 2 darab LFSR-re (Lineárisan Visszacsatolt Léptető-regiszteres Számláló) épül. A kódolás további ismertetésétől a dolgozat keretei és annak bonyolultsága miatt eltekintek.

A CSS működési mechanizmusa azonban hamar napvilágra került, és gyorsan kidolgozták a védelem feltörésének módszerét. *A 40 bites kulcsot bruteforce eljárással rövid idő alatt fel lehet törni*, illetve négy, vagy öt ismert kimeneti bájtból visszafejthető a titkosítatlan tartalom. *A Macrovision fejlesztésű Content Scramble System törésére elérhető a DeCSS nevű program, melyet az internetezők körében jól ismert Jon Johansen készített 15 évesen, mikor bevallása szerint elege lett abból, hogy a megvásárolt DVD-it nem tudja megnézni a DRM-et nem támogató számítógépén.*

A DeCSS-hez hasonló, rendkívül népszerű, és meglepő módon bizonyos ideig ingyenesen használható programot készített a SlySoft nevű cég. Termékük neve az AnyDVD, roppant beszédes. *Képes bármilyen DVD lemezzől eltávolítani a régió kódot, az analóg védelmet (Macrovision), a másolásvédelmi eljárásokat, a DVD lejátszás megkezdésekor átugorhatatlan részeket, valamint a menürendszert.*



2. ábra AnyDVD beállítások

Az alkalmazást készítő SlySoft további termékei a sokak által ismert és használt CloneCD, CloneDVD és CloneDVD Mobile.

3.4. A nyomtatott sajtó

A papír alapú tartalmak előállítói számára a helyzet annyiban tér el az előbb említett vállalatok sorától, hogy a nyomtatott tartalom digitalizálása sokkal hosszadalmasabb folyamat egy átlagember számára, mint egy CD tartalmának számítógépre mentése. Léteznek ugyan olyan eszközök, amelyek könyvek üzemi digitalizálására lettek kitalálva, azonban ezek nem gyakoriak a háztartásokban. Ennek oka lehet az eszközök ára, azaz a fix költség jelenti a legfőbb akadályt a másolás folyamatában. Másrészt a könyvtulajdonos számára csekély jelentősége van egy könyvdigitalizáló eszköznek, mivel könyvet olvasni kényelmesebb hagyományos formában, mint képernyőről. A papíron hordozott információ jelentős része kevésbé vonzó célpont a „hobbi kalózok” számára, akik profitorientáltság nélkül, csupán a hírnévért és a tiszteletért teszik közzé az interneten a szerzői jog által védett tartalmakat. Természetesen léteznek olyan felhasználók, akik szöveges termékek digitalizálására specializálódnak. Vannak olyanok is, akik nem a tisztelet, hanem a profit reményében szegik meg a szerzők jogi érdekeit, és digitalizálják a papír alapú tartalmat. Ezen két csoport miatt kényszerülnek a tartalom előállítók arra, hogy maguk is felkínálják a tartalmat digitális formában, és ezzel a fogyasztók számára értéket teremtsenek, és a kalózok piacát szűkítsék. Ezzel a lépésükkel azonban le is bontják a legnagyobb akadályt a tartalmuk digitális terjesztése előtt. A már digitalizált szöveges tartalom rendkívül könnyen elválasztható annak előállítójától, ráadásul a plagizált változatok felkutatása, és esetleges jogdíj-fizetésre kötelezése szinte lehetetlen feladat. Éppen ezért minden ezzel kapcsolatos informatikai megoldás a figyelem középpontjába szokott kerülni. A könnyű másolhatóság és leleplezhetetlen plagizálás miatt a *dokumentum csere legfőbb formátuma* az Adobe **Portable Document Formatja** (PDF) lett, mely alkalmas a dokumentummal kapcsolatos jogok korlátozására, illetve titkosítás alkalmazására, az illetéktelen olvasók kizárása érdekében. [32]

A PDF formátumon túl egyéb elektronikus-könyv formátumok és megoldások is születtek, ezek közül mégis a PDF vált de facto szabvánnyá. Jelenleg az ISO minősítés küszöbén áll.

[1]

A papír alapú tartalmak esetében kevésbé reaktív, mint inkább proaktív eljárás a digitális jogkezelő rendszerek alkalmazása. Az eddig tárgyalt kiadók, stúdiók és fejlesztő cégek termékeivel ellentétben a nyomtatott tartalmak nem másolásra kész állapotban kerülnek

terjesztésre. A nyomtatott tartalmak tulajdonosai ezért a DRM rendszereket elsősorban arra használják, hogy úgy léphessenek be az online piacra, hogy termékük eleve védve van.

A PDF szabvány lehetővé teszi, hogy egy dokumentumot ne lehessen kinyomtatni. Ezt a tulajdonságát a PDF létrehozásakor kaphatja meg.

A problémára például a Ghostscript nevű program a megoldás, mely kiiktatja a nyomtathatóság tiltását a PDF fájlokban.

3.5. A mintavételezett audió tartalmak

A különböző veszteséges hangtömörítési technológiák szintén az internet elterjedésével váltak a hétköznapi élet szerves részeivé. A legelterjedtebb ilyen formátumok az **mp3**, az **AAC** (Advanced Audio Coding) és a **WMA** (Windows Media Audio).

Az mp3 1995-ös megjelenése óta az egyik legnépszerűbb audióformátum. Megalkotásakor a fejlesztők nem gondoltak jogkezelési rendszer kialakításra, és mivel rendkívül népszerű rendszerről van szó, ennek pótlására nincs lehetőség. Egyes vállalatok megpróbálkoztak jogkezelő rendszert fejleszteni az mp3 szabványhoz, azonban ezek a megoldások nem terjedhettek el széles körben, mivel a legtöbb dekódoló eljárás nem támogatta ezeket.

A legnagyobb on-line zeneáruházak kezdetben úgy oldották meg ezt a problémát, hogy egyszerűen nem forgalmaztak mp3 formátumú tartalmakat. Megtehették, mivel a másik két legnépszerűbb eljárást szállító cég az Apple és a Microsoft saját fejlesztésű médiatípusában megoldotta a jogkezelés kérdését.

Így aztán, ha egy adat *AAC formátumban* áll rendelkezésre, akkor igen valószínű, hogy az az *Apple által kidolgozott „Fair Play” DRM* rendszerrel van kódolva. Amennyiben a fájlkiterjesztés *„wma”* vagy *„asf”*, akkor az adott fájl feltehetően a *Microsoft DRM* rendszerével van ellátva.

3.5.1. Apple FairPlay DRM

A FairPlay az Apple számára a Veridisc nevű vállalat által készített digitális jogkezelési eljárás. Az eljárást alkalmazza a QuickTime multimédia alkalmazás, megtalálható az iPhone-okban, iPod-okban és az iTunes alkalmazásban. Az Apple saját alkalmazásain kívül számos egyéb program képes az ily módon védett tartalom visszajátszására. Ilyen például a RealPlayer, a MediaCenter, és a Windows Media Player Classic. [24]

Valamennyi, az iTunes Store on-line zeneáruházból származó aac kiterjesztésű fájl a FairPlay eljárással kódolva áll rendelkezésre. Az ilyen fájlokat vásárlók biztosak lehetnek abban, hogy az általuk megvásárolt védett tartalmakat jogosulatlan felhasználók nem képesek lejátszani.

A FairPlay rendszerrel védett fájlok szabályos MP4 konténerek, kódolt AAC audió jelfolyammal. Az audió stream kódolásához AES algoritmust használ MD5 hash-ekkel keverve. *A kódolt jelfolyam dekódolásához szükséges mester-kulcs szintén kódolva található az MP4 konténerben. Azt a kulcsot, ami a mester-kulcs megszerzéséhez szükséges „user-kulcsnak” hívják.*

Minden alkalommal, mikor valaki megvásárol egy felvételt az áruházban egy új, véletlenszerű kulcsot generál a rendszer, amivel elkódolja a felvétel mester-kulcsát. Valamint ezt a kulcsot eltárolja a felhasználó személyes profiljával együtt az Apple szerverén és továbbítja azt az iTunes rendszernek. Az iTunes ezeket a kulcsokat a saját titkosított kulcstárában tárolja. Felhasználva ezt a kulcstárat, az iTunes képes visszakeresni a szükséges user-kulcsot, a hozzá tartozó master-kulcs dekódolásához. A master-kulcs segítségével aztán képes dekódolni az AAC jelfolyamot, és lejátszani a felvételt.

Mikor egy felhasználó bejelentkezik egy új számítógépről, az iTunes küld egy egyedi gép azonosító kódot az Apple szerverének. Ettől kezdve ezen a gépen is megkapja az összes tárolt kulcsot, amik a személyes profiljában találhatók.

Ezzel a módszerrel az Apple képes korlátozni, hogy egy felvétel mennyi számítógépen legyen lejátszható.

Az iPodok szintén saját kulcstárral rendelkeznek. Minden alkalommal amikor egy felvételt másolnak az iPod-ra az iTunes gondoskodik róla, hogy a megfelelő user-kulcs is átkerüljön a lejátszóra. Így biztosítva, hogy a védett AAC audió tartalmak mindig lejátszhatók legyenek.

A FairPlay rendszer nem alkalmas a fájlok másolásának megakadályozására. Kizárólag az audió tartalomhoz való jogosulatlan hozzáférést hivatott korlátozni.

Jon Johansen – akit a DVD lemezek védelmére fejlesztett CSS rendszer feltörése kapcsán már említettem – volt az eső, aki rájött, hogyan lehet megkerülni a FairPlay védelmi rendszerét.

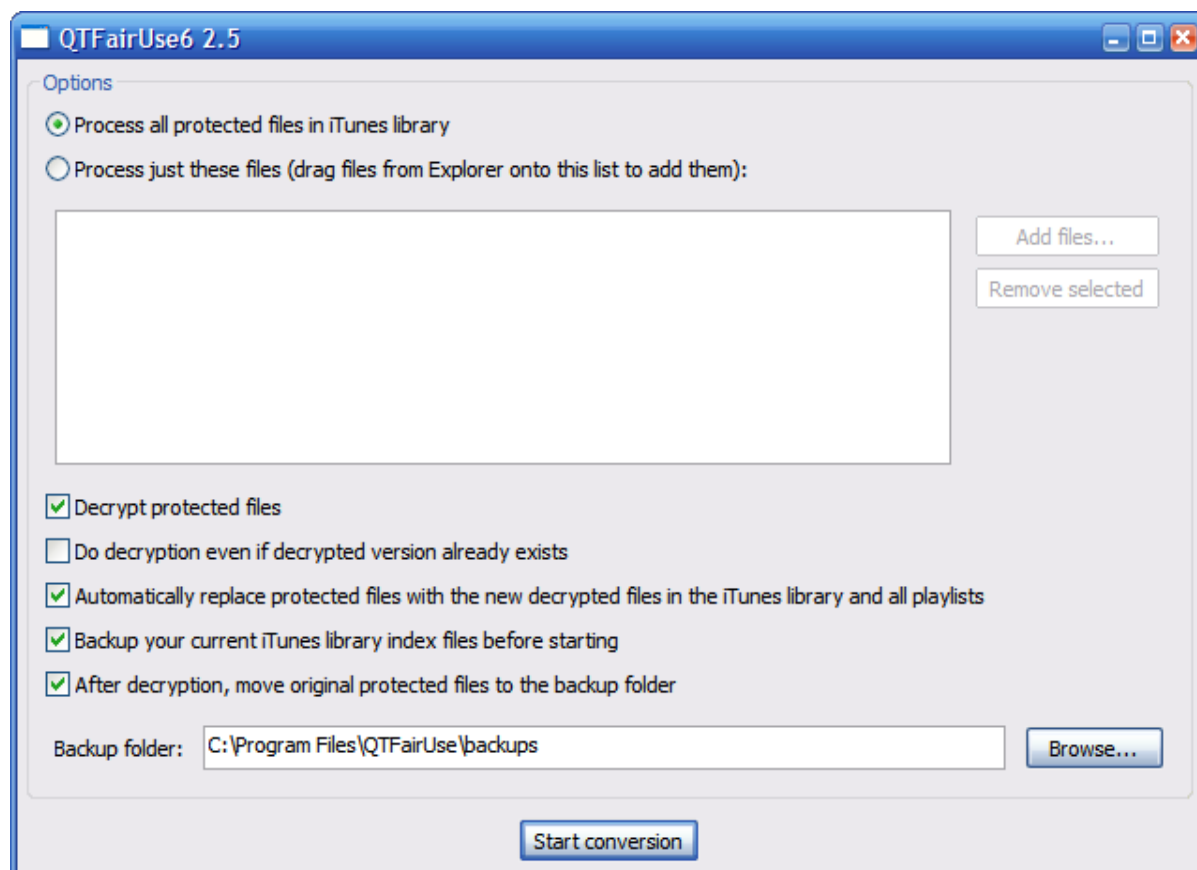
A QTFairUse névre keresztelt programjával képes kinyerni a védett fájlból az audió tartalmat, és azt egy új „csupasz” AAC fájlként tudja menteni. Azonban sok lejátszó nem támogatta az ilyen „csupasz” fájlokat, ezért kénytelen volt más típusú tömörítést alkalmazni a kimeneten.

Ezt követően Johansen visszafejtette a FairPlay teljes algoritmusát, és elkészítette azt az eljárást, ami teljes egészében eltávolítja a kódolást anélkül, hogy újrakódolná az eredeti AAC

jelfolyamot.[29]

Ezt az eljárást jelenleg is használja a VLC Media Player FairPlay DRM-mel védett tartalmak lejátszása esetén.

Néhány nappal az iTunes 7.0 verziójának megjelenése után, kísérleti jelleggel már elérhető volt a QTFairUse 2.3 változata, ami bármilyen formátumban képes volt menteni a védett audio tartalmakat.



3.Ábra QTFairUse6 2.5 Windows XP környezetben

Jon Johansen a maga által készített dekódoló eljárást **DeDRMS**-nek nevezte el. Az ő nevéhez kapcsolódik még a FairKeys nevű alkalmazás, ami az Apple kiszolgálóról hivatott megszerezni a szükséges kulcsokat a DeDRMS számára.

Két közös jellemvonása van ezeknek az alkalmazásoknak. Az egyik, hogy a user-kulcsot az Apple szerveréről, az iTunes, vagy az iPod kulcstárából szerzi, ezzel garantált, hogy a dekódolandó fájl legálisan került a felhasználó birtokába. A másik, hogy változtatás nélkül megőrzi a felhasználó specifikus metaadatot az MP4 konténer belsejében, így egyértelműen

azonosítható az a felhasználó, aki az adott tartalmat megvásárolta, és dekódolta annak DRM védelmét.

Nagy valószínűséggel ezek a roppant megfontoltságról tanúskodó tények menthették meg a fiatalembert a hosszú börtönévektől.

3.5.2 Windows Media DRM

A Windows Media DRM egy digitális jogkezelő szolgáltatás a Windows Média platformon, mely arra szolgál, hogy védje a média tartalmakat az illetéktelen felhasználástól mind az IP hálózatok felett, mind pedig a számítógépek és más média-lejátszó eszközök között.

A WMDRM részei:

- A Windows Media Rights Manager (WMRM) szoftverfejlesztő készlet, mely felelős azért, hogy becsomagolja a tartalmakat és kiállítsa a licenceket.
- A Windows Media Format SDK (WMF SDK) amely lefordítja a Windows alkalmazás számára megfelelő DRM támogatást és a megfelelő formátumot.
- A Windows Media DRM for Portable Devices (WMDRM-PD) az offline hordozható eszközökön történő lejátszást támogatja.
- Valamint a Windows Media DRM for Network Devices (WMDRM-ND) lehetővé teszi a védett tartalmak stream-elését a helyi hálózati eszközökön.

A Windows DRM rendszere az elliptikus függvény titkosítású kulcs cserét, DES blokk titkosító algoritmust, MultiSwap blokk titkosítást, RC4 folyam titkosítást, és SHA-1 hash függvény kombinációját alkalmazza a védett tartalom előállítására.

A rendszer úgy lett kialakítva, hogy abban az esetben, ha feltörik a védelmet, a kliensoldali alkalmazások módosítása nélkül lehessen módosítani az algoritmuson.

A Windows Media jogkezelő becsomagolja a digitális médiafájlt. A becsomagolt fájl titkosítva van, és „kulcs” zárja le. *A kulcsot titkosított licenc tárolja, amelynek terjesztése külön történik.* (Ez a jellemző kizárólag a Windows Media jogkezelő sajátja.) A terjesztő további adatokkal is kiegészítheti a digitális médiafájlt, például megadhatja azt az URL-címet, ahonnan a licenc beszerezhető.

A csomagolt fájl elhelyezhető webhelyen, ahonnan letölthető; közvetíthető digitális médiakiszolgálóról; terjeszthető CD-lemezen, valamint elküldhető elektronikus levélben a felhasználóknak. A Windows Media DRM lehetővé teszi a felhasználók számára, hogy a másolásvédett digitális médiafájlokat elküldjék az ismerőseiknek is.

A tartalomszolgáltató kiválasztja azt a licenckezelő központot, amelyik a licencekben megadott jogokat és szabályokat tárolja, és megvalósítja a Windows Media jogkezelő

licencszolgáltatásait. A licenckezelő központ szerepe a licencet kérő felhasználói kérések hitelesítése. A digitális médiafájlok és a licencek terjesztése, illetve tárolása elkülönítetten történik, leegyszerűsítve ezzel a teljes rendszer kezelését.

A csomagolt digitális médiafájlok lejátszásához a felhasználónak először licenckulcsot kell beszereznie. A licenckérési folyamat automatikusan elkezdődik, amikor a felhasználó megkísérel a csomagolt digitális médiafájl megszerzését, lekéri az előzetesen továbbított licencet, illetve első alkalommal lejátssza a fájlt. A Windows Media jogkezelő regisztrációs lapra irányítja a felhasználót, ahol annak különböző adatokat kell megadnia vagy díjat kell fizetnie, illetve a háttérben lekéri a licencet a licenckezelő központtól.

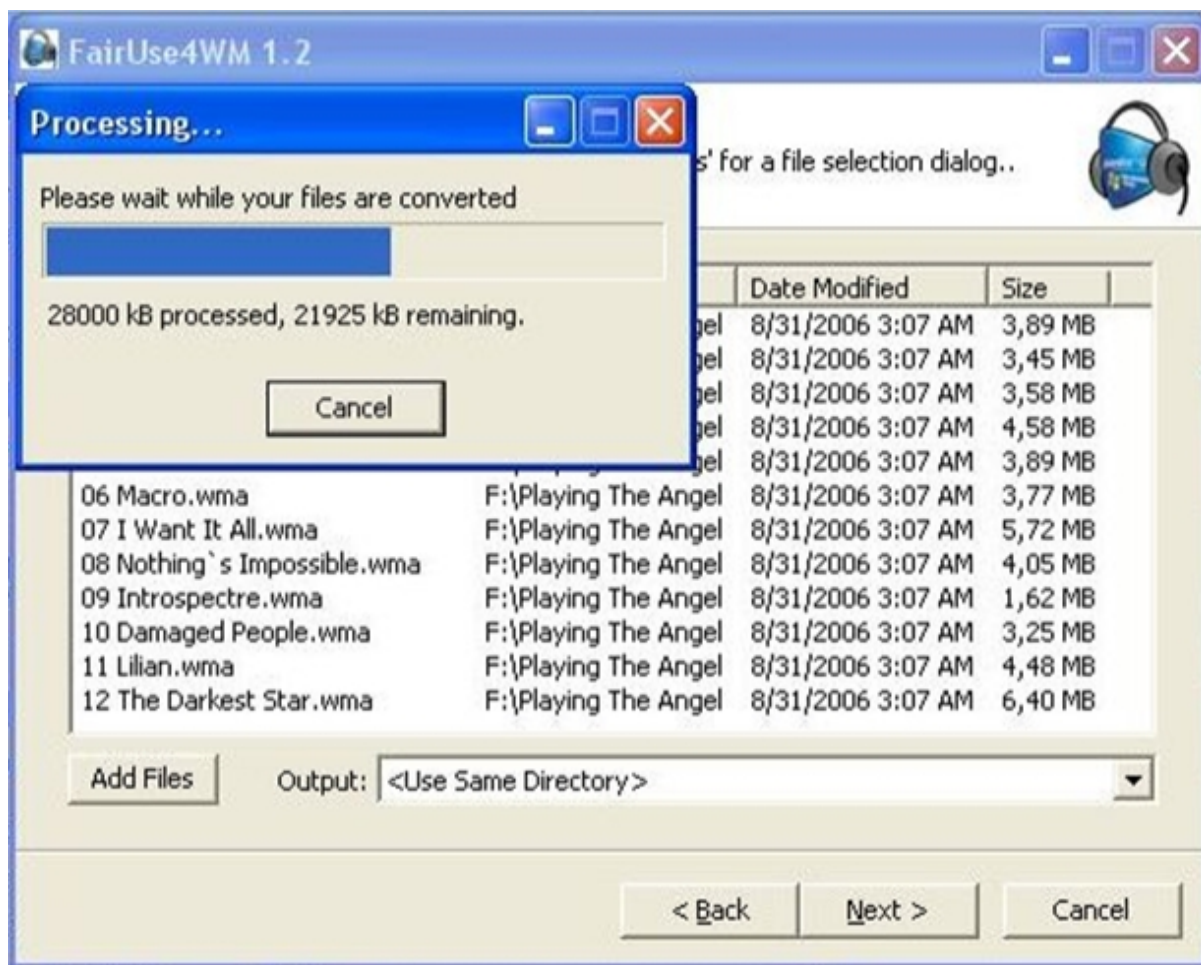
A digitális médiafájl lejátszásához a felhasználónak olyan lejátszóra van szüksége, amely alkalmas a Windows Media DRM használatára. *A felhasználó a licenccben megadott engedélyek és előírások szerint játszhatja le a fájlt.* A licencek különböző feltételeket tartalmazhatnak, előírhatják például a kezdési és a befejezési időpontot, illetve meghatározott mennyiségű műveletet engedélyezhetnek. Az alapértelmezés szerinti jogok lehetővé tehetik például a digitális médiafájl meghatározott számítógépen történő lejátszását, valamint a fájl lejátszóeszközre történő átmásolását. A licencek azonban nem ruházhatók át. *Ha a felhasználó a csomagolt digitális médiafájlt elküldi az ismerősének, annak saját licencet kell beszereznie a digitális médiafájl lejátszásához. Ez a számítógépenkénti engedélyezési rendszer garantálja, hogy a csomagolt digitális médiafájl csak azon a számítógépen legyen lejátszható, amelyik megkapta az ehhez szükséges licencet.*

A Microsoft a következő hordozhatóeszköz-gyártó cégek támogatását jelentette be: Casio, Cirrus Logic, Creative, CVC Networks, Diamond, Digisette, DnC Tech, e.Digital, Hewlett Packard (Compaq), Hitachi, I-Jam, Iomega, Intel, MIPS Technologies, Nike, NTT DoCoMo, Olumpus, Panasonic, Sanyo, Sensory Science, Sigmatel, Sonic Blue, Sony, Texas Instruments és Thomson/RCA. A vezető chipgyártók támogatásával a Windows Media formátum (a Windows Media hangkodekkel és a Windows Media jogkezelővel együttesen) a legszélesebb körben támogatott, nem MP3-típusú formátummá vált. [18]

Leleményes programozóknak a rendkívül kevés rendelkezésre álló technológiai információ ellenére, a WMDRM legfrissebb verzióihoz (Windows Media DRM 10 és 11) - melyek szerves részei a PlaysForSure elnevezésű kampánynak – is sikerült olyan alkalmazást készíteni, melynek segítségével megkerülhető a Microsoft megoldása.

A megoldás neve FairUse4WM.

A FairUse4WM nem töri fel a DRM kódolását. A működéséhez elengedhetetlen, hogy érvényes licenccel rendelkező fájl jegyen a felhasználó birtokában. Ebből a fájlból nyeri ki a program a kódolatlan tartalmat, amit aztán az eredetivel megegyező formátumban képes menteni. A program, a drmdbg nevű szoftver GUI (Graphical User Interface) változata.



4. Ábra FairUse4WM 1.2 Microsoft Windows XP operációs rendszerben

3.6. Blu-ray Disc és HD DVD

A két új kék lézeres szabvány közti egyik lényeges különbség az alkalmazott másolás védelmi rendszer (CPS). A HD DVD szabvány megalkotói egyedül az AACCS-t választották, míg a Blu-ray esetén az AACCS mellett két további biztonsági réteget is alkalmaztak ezek a BD-ROM Mark és a BD+.



Overview of BD-ROM format

		BD	HD-DVD
Application	Advanced Menu, Network	Java (BD-J)	iHD
	Basic menu	BD navigation (HDMV)	HD DVD-Video
	Video Codec	MPEG2 MPEG-4 AVC VC1	MPEG2 MPEG-4 AVC VC1
	Audio Codec	LPCM Dolby DTS	LPCM Dolby DTS
	Multiplex system	Transport Stream	Program Stream
CPS	Basic CPS system	AACS	AACS
	Security VM	BD+	N/A
	Physical protection	BD-ROM mark	N/A
File system		UDF V2.5	UDF V2.5
Physical	Error Correction	Long Distance method	Product Code method
	Signal Processing	Limit Equalizer method	PRML method
	Physical Structure	0.1mm cover layer	0.6mm

5. ábra a BD-ROM és a HD DVD felépítése

Az **Advanced Access Control System** biztosítja a BD-ROM audio és videó adattartalmak védelmét. Általánosságban ez határozza meg az ezen eljárással védett tartalmak kezelésének szabályait. Az AACCS 128 bites kulcsú titkosítást használ a lemezek azonosítására. A technológia révén lehetőség nyílik a kompromittált eszközök letiltására és a fejlettebb lejátszó azonosításra. Lehetőséget nyújt továbbá az engedélyezett másolásra, például az otthoni hálózaton belüli lejátszásra vagy hordozható lejátszóra másolásra.

Az *Image Constraint Token (ICT)* az AACCS analóg videó kimenetre alkalmazott része. Ez az

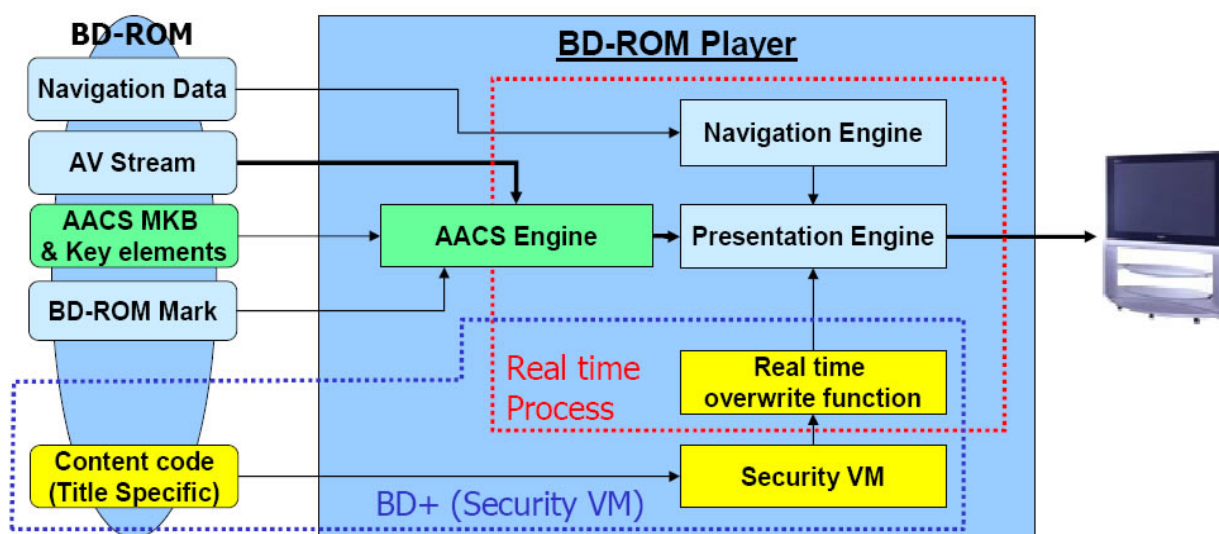
eljárás lekonvertálja az analóg kimeneten lejátszott HD videó jelet maximum 960x540-es felbontásúra. Az ICT nem kötelezően alkalmazott eljárás, a mostanáig megjelent HD anyagok (HD DVD és Blu-ray) még nem tartalmazzák. Amennyiben egy BD-ROM kiadvány támogatja az ICT-t, azt fel kell tüntetni a borítón.

További analóg védelmet biztosít az AACS, a *Digital Only Token* technológia. Ez képes megakadályozni, hogy a videó tartalom a lejátszó analóg csatlakozóin keresztül megjeleníthető legyen, de felkészítették az újszerű üzleti modellben történő felhasználásra is, amely merőben más, mint a hagyományos videó árusítás. A videó kiadványok a filmszínházakban játszott verziótól a HD mozi előzetesig terjedhetnek. A Digital Only Token a végleges AACS tervezet része, amely 2006 második negyedévétől elérhető.

Az a AACS tartalmaz egy audió vízjelet is. Ezt a nem hallható jelet a tartalom-szolgáltató alkalmazhatja az audió sávoknál. Ez az eljárás nem támogatott a jelenlegi eszközökben, de várhatóan része lesz a végleges AACS rendszernek.

Végül mindkét tábor elhatározta, hogy 2013-ra megszűnik az analóg jeltovábbítás támogatása az USA-ba és Japánban. Az úgynevezett 'Analog Sunset' várhatóan 2010-ben kezdődik, mikortól az analóg kimenet SD váltósoros módra lesz korlátozva (kompozit, S-Video, 480i komponens).

A fenti tulajdonságokat a HD DVD és a Blu-ray formátum is támogatja. De mint már jeleztem a BDA felhasznál két további biztonsági réteget a BD-ROM esetében ezek a BD-ROM Mark és a BD+.



6. ábra A Blu-ray működési mechanizmusa

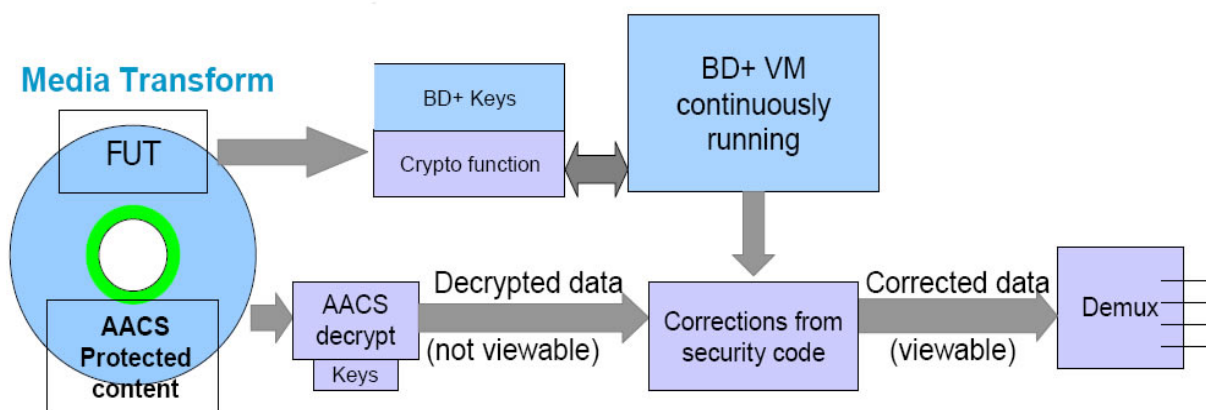
A ROM-Mark egy fizikai réteg, amely azt hivatott megakadályozni, hogy a professzionális hamisítók képesek legyenek másolni a BD-ROM lemezeket. A ROM-Mark megakadályozza a BD-ROM kiadványok írható lemezekre történő másolását, ez *egy analóg szintű technológia a bitről bitre másolás ellen*. A ROM-Mark használatához egy speciális berendezésre van szükség a lemez mastering-kor.

A BD+ technológia

A BD-ROM lejátszók tartalmaznak egy kis virtuális gépet (VM, BD+ Content Code interpreter), hogy biztosítsák a futtatási környezetet a BD+ Content Code működéséhez. Ezenkívül ez a VM lehetőséget ad a kiadóknak, hogy kiadványonként különböző BD+ Content Code-ot használjanak.

A virtuális gép (VM) egy kicsi BD+ Content Code értelmező mely 100 sorból áll és 60 utasítást ismer, így az erőforrás igénye csekély.

A BD-ROM lemezek lejátszásakor a VM lefuttatja a Content Code-ot, hogy biztonsági ellenőrzést hajtson végre és engedélyezi a lejátszást a legitim lejátszókon. A biztonsági kód a lejátszás során végig fut, szerepe a korrupt adatok kijavítása és a látható tartalom előállítása. A média transzformáció valós időben zajlik a Security VM kimenetét felhasználva.



7. ábra A Blu-ray szerzőijog-védelmi mechanizmusa

A BD+ három fázisból áll:

- Transform code (minden esetben használható)

Felcserél bizonyos AV adatokat külön előállított AV adatokkal. Például az ilyen AV adat rész a lemezen nem adja vissza az eredeti tartalmat a content code-ot futtató security VM javítása nélkül. Ezzel az eljárással azonosítható az esetlegesen illegálisan terjesztett tartalmak forrása.

- Alapvető ellenintézkedések (mikor egy törést megerősítettek)

Mikor egy törést megerősít az érintett lejátszó gyártója, a tartalom-szolgáltatók kifejleszthetik az ezt kiküszöbölő BD+ Content Protection kódot.

- Fejlett ellenintézkedések

A BD+ képes natív kódot futtatni a lejátszón. Ezáltal lehetőség nyílik az egyedi válaszlépésre a törések esetében. A BDA szerint a BD+ rendszer sikeres megkerüléséhez a kalóznak meg kell kerülni az AV tartalom biztonsági rendszerét (pl.: kinyerni az AACS kulcsokat) és meg kell kerülniük a kiadvány specifikus biztonsági kódokat (visszafejteni a biztonsági kódot).

A BD+ Content Code csak akkor fut, mikor a lemez a lejátszóban van, kivétele után a lejátszó visszaáll a betöltése előtti állapotra.

A BD+ kulcs képes kriptográfiailag megkülönböztetni a feltört lejátszókat a nem feltörtektől így a BD+ Content Code csak az azonosítót meghamisító lejátszókon fut.

Első ízben, 2006 júliusában keltek napvilágra olyan hírek, miszerint megkerülhető mind a HD DVD, mind pedig a Blu-ray Disc védelmi rendszere.

A német c't számítástechnikai magazin munkatársainak igen egyszerű eljárással sikerült megkerülniük ezt a védelmet.

Amint azt megfigyelték a Windows XP alatti első szoftveres lejátszó megengedi a képernyőmentés készítését teljes felbontásban a futó filmekről. Egyszerűen nyomva kell tartani a Print Screen billentyűt, amíg a lejátszás tart. Az ilyen képernyőmentés funkcióval lehetővé válik teljes HD tartalmak automatikus felvétele HD DVD vagy Blu-ray lemezekről. Számításaik szerint a mai PC-k teljesítménye elegendő megfelelő minőségű, és mennyiségű felvétel készítésére. Amint a képről-képre mentés elkészült, könnyedén összefűzhető mozgóképpé, valamint mellékeverhető a külön grabbelt hang, így az eredeti anyag teljes értékű másolatát kapjuk.

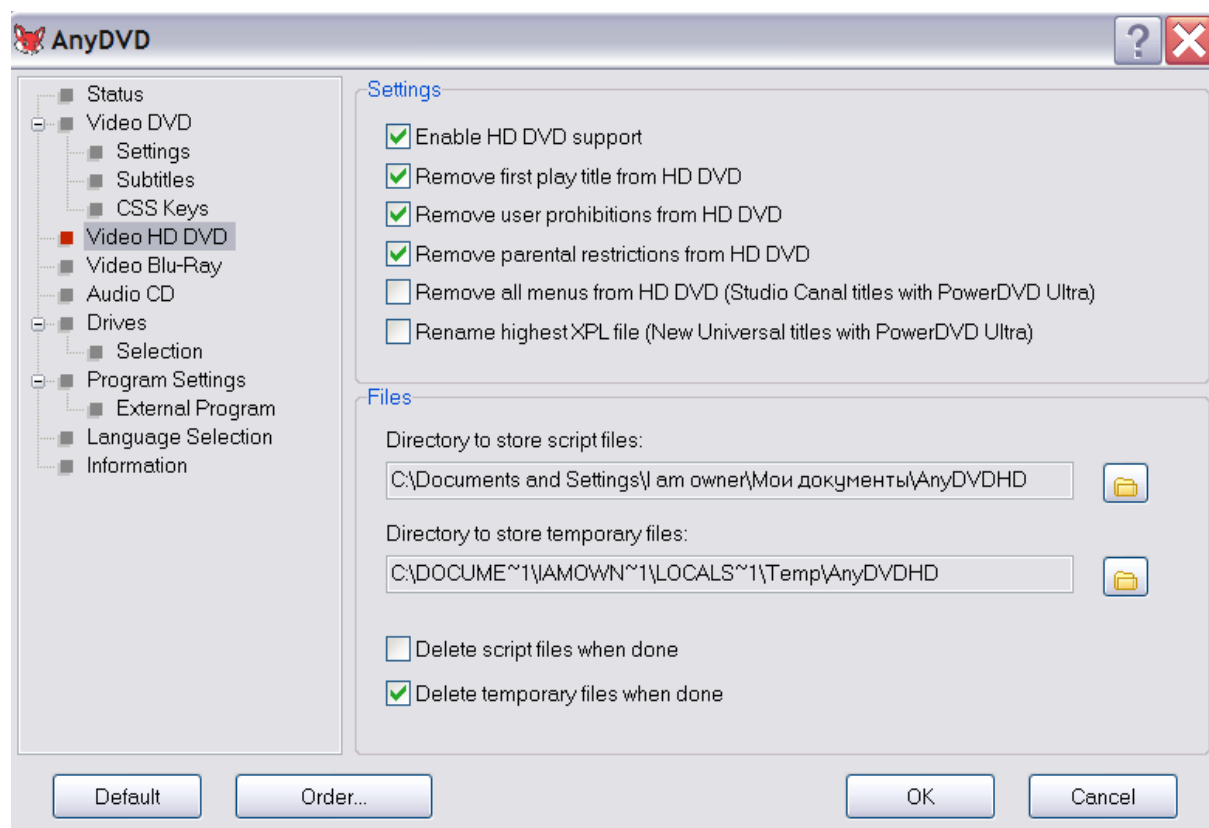
Ez a másolásvédelmi lyuk megtalálható mind a Sony első Blu-ray meghajtós PC-jében a Vaio VGC RC 204-ben, mind a Toshiba HD DVD meghajtóval szerelt Qosimo G30 notebookjában. Mindkét esetben az Intervideo WinDVD OEM verziója a szoftveres lejátszó.

Feltörés: 2007 február 11-én egy fórumon bejelentette az arnezami nevű blogger, hogy az egyik Windows-os lejátszó segítségével kinyerte eredeti lemezéből a processing- és média-kulcsokat, valamint a Volume ID-t. Ennek a három adatnak a segítségével az összes eddig megjelent HD DVD és Blu-ray lemez lemásolható.

Saját elmondása szerint rengeteg időt töltött az AACS dokumentációjának

tanulmányozásával, mely mindenki számára hozzáférhető. Szoftveres lejátszóprogramot alkalmazott, melynek a nevét nem árulta el. Mint a legtöbb esetben, itt is a számítógép memóriájából sikerült visszafejtenie a dekódoláshoz szükséges kulcsokat. A memória vizsgálatára a WinHex nevű memória dump programot használata. Legelőször a Volume ID-t fedezte fel, majd hosszú ideig nem jutott tovább. Saját elmondása szerint kezdett komolyan aggódni, hogy nem jár sikerrel. Számos, különböző pillanatban végezett mintavétel sem vezetett újabb eredményre, azonban egyik alkalommal különös dologra lett figyelmes. A WinHex hibaüzenettel tért vissza a feladat befejezése előtt, miszerint a memória megváltozott. Összevetette az aktuális mentést számos korábbival, és érdekes módon olyan memóriaterületre lett figyelmes, mely korábban foglalt volt. Ekkor döbbsen rá, hogy az általa keresett kódsorozat nem marad a memóriában, hanem csak ideiglenesen található meg benne. A felfedezés eredménye a processing kulcs lett. Ennek birtokában már szinte „gyerekjáték” volt megszerezni a media kulcsot, és teljes egészében védtelenné vált a DVD.

Ezeket a kódokat felhasználták a már korábban ismertetett AnyDVD nevű program 6.3.1.7. verziójában az AnyDVD HD-ben, mely könnyedén megszabadítja az eddig kiadott HD DVD és Blu-ray lemezeket a védelmüktől.



8. ábra Az AnyDVD nevű alkalmazás DVD beállításai Windows XP környezetben

3.7. A felhasználói élmény

Az eddigi fejezetekben a DRM rendszereket működésük bemutatásán keresztül vizsgáltam, melyeket rendszeresen példákkal támasztottam alá. Ebben a fejezetben a DRM rendszerekkel kapcsolatos fogyasztói élményeket vizsgálom.

Az HBO kábeltelevízió hálózat amerikai honlapja szerint az HBO és a Cinemax adásainak rögzített változatáról nem szabad másolatot készíteni. A másolatkészítés tilalma az analóg eszközökre is vonatkozik, azaz a hagyományos mágnesszalagos videófelvevő eszközökre is. [15]

A Microsoft Windows Vista operációs rendszeren lejátszott un. prémium tartalmak esetén az operációs rendszer a tartalmat védő DRM utasítására a számítógép szabványos, analóg hangkimenetét letiltja.

Az analóg jelek problémája, hogy azok viszonylag egyszerűen rögzíthetők, digitalizálhatók, majd az analóg-digitális konverzió után minőségromlás nélkül másolhatók. A jelenséget „analóg lyuknak” hívják. Az analóg lyuk betömésének lehetséges módja, ha az analóg ki- és bemenet szabványa lehetővé teszi a jogvédett tartalmak megkülönböztetését, és a megkülönböztetést az eszközök figyelembe is veszik. Továbbá, ha a megkülönböztetést a szabvány nem teszi lehetővé, úgy azt a ki- és bemenetet az eszköz letiltja.

A Windows Vista operációs rendszer a videótartalmat védő DRM utasítására képes letiltani az S/PDIF audió portot, mivel a szabvány nem alkalmas az adatfolyamról történő másolatkészítés megtiltására.

Az HBO által alkalmazott CGMS-A (Copy Generation Management System Analogue) rendszer képes megjelölni a videokazettán található analóg tartalmat, és ennek a tartalomnak a másolása nem lehetséges, amennyiben a másoló eszköz figyelembe veszi a CGMS-A másolásvédelem jelölését. Ha az eszköz nem ismeri a CGMS-A rendszert, a képi megjelenítés élvezhetetlenné válik.

A High Definition tartalmak és az azokat lejátszó eszközök elterjedéséig az analóg jelek fontos szerepet játszanak. A mindennapi életben a műholdon, kábelon, földi adón át vagy éppen DVD-n érkező digitális jelfolyamot a lejátszó eszköz analóg jellé alakítja, hogy a televízió készülékek meg tudják jeleníteni. A digitális televíziózás korszakának kezdetén sem lesz ez másként. A régi televíziók és az Set-Top-Box (olyan készülék mely a digitális tévéadást analóg formába konvertálja) közötti jelfolyam tipikusan analóg, azaz minden analóg

port letiltása nem lehet hatékony megoldás egyelőre, hiszen számos potenciális fogyasztó válna elérhetetlenné az analóg lejátszási lehetőség nélkül. Hasonló okból nem lehetséges az sem, hogy az analóg jelfolyamot tömegesen ellássák másolásvédelmi jellel, hiszen a technológiát nem ismerő lejátszók esetén az eszköz nem lenne képes megjeleníteni a megvásárolt tartalmat.

A probléma megoldódásának felgyorsítására született törvényjavaslat Amerikában a „digitális átvitel tartalomvédelmi törvény”, azaz a Digital Transition Content Security Act (DTCSA). A törvény megtiltja, hogy bárki „gyártson, importáljon, a nép számára felajánljon, elérhetővé tegyen vagy más módon forgalmazzon” olyan analóg videó eszközt, mely nem veszi figyelembe a jelfolyamba ágyazott másolásvédelmi megjelölést.

Az „analóg lyuk” betömésére létezik törvény, a DMCA. A Digital Millennium Copyright Act egy 1998-ban beiktatott amerikai törvény, célja a digitális szerzői jogok megsértése elleni fellépés. A DMCA a szellemi tulajdonjogokkal kapcsolatos problémák digitális vonzataival foglalkozik, és kifejezetten kiemeli az interneten történő szerzői jogsértést. *A törvény többek között lehetőséget ad a másolásvédelmi technológiák kikerülésének tiltására. A másolásvédelmet még saját használatra készülő másolat esetén is tilos feltörni, illetve a másolásvédelem feltörésének mechanizmusát is tilos továbbadni. A DMCA, és európai párja, az EUCD (az EUCD az Amerikai Egyesült Államokban érvényes DMCA Európai változata) megtiltja az olyan eszközök forgalmazását, birtoklását, mely a digitális jogkezelő rendszerek megkerülésére szolgál.* Az EUCD direktíva országonként eltérő módon lett implementálva a helyi környezetbe, így egyes, főként északi országokban a DRM rendszereket megkerülő eszközök birtoklása nem jogsértő.

A digitális kódolások egyszerűen beépíthetők az eszközökbe. A tartalomszolgáltatók így bátrabban vesznek igénybe digitális jogkezelő rendszereket, hiszen a digitális eszközök gyártóinak is érdeke, hogy a szolgáltatók tartalmát az eszköz felhasználója meg tudja nézni, hallgatni. Amennyiben egy eszközgyártó nem kívánja a jogkezelő rendszer utasításait betartani, úgy a DRM-szállító nem bocsátja rendelkezésére a szükséges technológiai specifikációt a védett tartalom visszakódolására. Az eszköz felhasználója pedig azt tapasztalja, hogy a tartalmat nem tudja elérni. Az eszközgyártók számára a választás tehát az, hogy a felhasználói számára nem biztosítja a megtekintés lehetőségét, vagy biztosítja, de akkor a tartalomszolgáltató szabályai szerint. A tartalomszolgáltató szabályai pedig a megszokott fogyasztói élményhez képest akár értécsökkenéssel is járhatnak.

A DRM rendszerek megtervezhetők úgy is, hogy a jogkezelési szabályt a tartalomszolgáltató utólag is módosíthassa. Pontosan ez történt a TiVo (Amerikában rendkívül népszerű Digitális Videórögzítő eszköz) tulajdonosaival. A TiVo kénytelen volt alkalmazkodni a már említett Macrovision cég szabályaihoz, és be kellett vezetnie a másolásvédelmi rendszert. A TiVo eszköz gyártója számára a kérdés az volt, hogy szeretne-e továbbra is Macrovision licenccel rendelkezni, és ennek megfelelő tartalmat lejátszani, vagy az egyszeri lejátszásra engedélyezett Macrovision tartalmak egyszer sem lesznek lejátszhatók az eszközein.

A játékszabályok módosításának hatására számos felhasználó tapasztalta, hogy a távolléte alatt felvett műsorokat hazaérve nem tudta megnézni. Voltak olyan felhasználók, akik a TiVo előfizetésüket mondták le a másolásvédelem bevezetése miatt. Habár a másolásvédelem bevezetése nem az eszközgyártó közvetlen érdeke volt, a felhasználók egy része mégis a TiVo készítőjét okolta.

A menet közben változó játékszabályok nem csak a TiVo esetében fordultak elő. Az Apple is változtatott a hozzáférési szabályokon, amikor az iTunes szoftverének új verzióját kiadta. A meghatározott sorrendben összeállított zeneszám listát eleinte 10 alkalommal lehetett CD-re menteni, majd az új verzió ezt 7 alkalomra korlátozta. Ennek az eljárásnak a korlátozása mellesleg teljesen értelmetlen, épp ezért sem az alkalmak növelése, sem az alkalmak csökkentése nem változtat különösképpen a helyzeten, hacsak 0-ra nem csökkentik, azaz megtiltják a CD-re mentés lehetőségét. Ha legalább egy alkalommal CD-re menthető egy zenekollekció, akkor a CD-ről bármikor készíthető további másolat, mert az Apple nem látja el másolásvédelemmel a CD-ket. Mégis, az elméleti lehetőség ott van a szoftverkészítő kezében, akit a tartalomszolgáltatók és tulajdonosok bármikor kötelezhetnek a szabályok szigorítására.

„Hasonló eset történt, amikor a RealNetworks cég Harmony nevű szoftvere lehetővé tette, hogy a RealNetworks RealRhapsody online áruházában vásárolt zenét le lehessen játszani iPodon. A Harmony szoftver a Real által használt Helix-DRM-et FairPlay kompatibilissé konvertálta, amelyet az iPodok le tudnak játszani. Az Apple a következő iPod firmware frissítéssel elérte, hogy a lejátszó ne játsszon le a konkurens cég boltjából vásárolt zenét.”

(Wikipedia – iTunes Store)

A DRM használata ebben az esetben nem csak arra szolgált, hogy a másolásvédelmen túl az Apple a fogyasztókat lekösse, hanem hogy a konkurens szolgáltatások fogyasztóit kizárja. A lekötés általános jelenség a zárt rendszerű DRM-ek esetén. Ez a helyzet az Apple FairPlay és

az iTunes-iPod páros esetében, a Sony OpenMG/ATRAC3 és a Sony mp3 lejátszók esetében, valamint a WMDRM és a Zune esetében. Az utóbbi esetében a helyzet annyiban újszerű, hogy a Microsoft nem egyszerűen a konkurenciát zárta ki, hanem saját felhasználóit is. A Microsoft mp3 lejátszója – a Zune – ugyanis nem képes olyan zenét lejátszani, amelyet előzőleg a Microsoft MSN áruházából vásárolt meg a felhasználó, és amely zenét a Microsoft PlaysForSure DRM rendszer védi.

A Mr. & Mrs. Smith amerikai film DVD-jét Németországban a Settec nevű cég Alpha- DVD protection DRM rendszerével látták el. A DVD beolvasásakor a felhasználók előtt egy hosszú végfelhasználói licencszerződés (EULA) szövege jelent meg, melyet a DVD lejátszáshoz el kellett fogadni. A szöveg felhívta a felhasználó figyelmét, hogy a szoftver „ártalmatlan” változtatást fog eszközölni az operációs rendszeren. Német fórumokon a felhasználói visszajelzések korántsem ártalmatlan hatásokról adtak számot. Optikai és virtuális meghajtók egyaránt elérhetetlenné váltak a felhasználók gépén. A Heise on-line szerkesztőségében feltelepítették a DVD-t védő DRM rendszert, és számos problémájuk akadt ezután a számítógépek CD/DVD meghajtóival. Az EULA felhívta a figyelmet arra is, hogy a DVD-t számítógépeken „általában” nem lehet lejátszani. Azonban a DRM rendszer megkerülhető volt. Amennyiben a felhasználó kikapcsolta az automatikus lejátszás (Autoplay) funkciót, vagy ha az EULA olvasása alatt egy lejátszóprogramot elindított, majd a film zavartalan megnézése után elutasította a licencszerződést, a számítógépre nem telepedett fel a DRM. A védelem nem érintette a nem-Windows alapú operációs rendszereket sem.

Ugyanígy a legális példányt megvásárló felhasználók jártak rosszul a Sony egyes CD-ivel. A CD-ket védő XPC nevű DRM rendszer olyan technikát használt az illegális másolás megakadályozása érdekében, amely jellemzően a hackerek eszköztárában szerepel. A figyelmeztetés nélkül települő DRM rendszer kitudódása után jelentek meg kártékony programok, amelyek a rendszert kihasználva fertőzték a felhasználók gépeit. Azok, akik nem vásárolták meg a CD-t, hanem inkább letöltötték a tartalmát, nem tették ki magukat a DRM rendszer veszélyének.

A legális vásárló problémája, hogy a jogszerűen megszerzett termék problémákat okoz számára. A Microsoft-partner zeneáruházból jogszerűen megvásárolt zenét a Microsoft Zune lejátszója nem játssza le, de illegálisan letöltött zenét lejátszik. A Mr. & Mrs. Smith német nyelvű DVD-t megvásárló felhasználó számára problémákat okozhatott a védelmi rendszer, míg egy hozzáértő felhasználó egyszerűen ki tudta iktatni a védelmet, és az internetről

letölthető változat mentes volt ilyen veszélyektől. A Sony BMG által forgalmazott bizonyos CD-k vásárlói az újságokból értesülhettek arról, hogy számítógépük veszélynek van kitéve, mert a CD, amiért pénzt fizettek, bizonyos értelemben megfertőzte a számítógépüket.

Az internet világában a bizalom megtartása elsődleges feltétel a sikeres üzleti működés fenntartásához. Hogyan lehet bízni a kiadókban, terjesztőkben, ha képesek bármit megtenni, amire a technika lehetőséget nyújt nekik? A bizalom problémájára az egyik megoldás a trustmarkok megjelenése volt. A trustmark emblémával rendelkező vállalatok megfelelnek a trustmark által megkövetelt feltételeknek. A TRUSTe esetében ez azt jelentette, hogy a vállalat nem készít profilokat a felhasználóktól szerzett adatokat felhasználva. 1999-ben kiderült, hogy a TRUSTe minősítéssel rendelkező RealNetworks zeneszoftvere adatokat gyűjtött az akkor 13,5 milliós felhasználó bázisáról. A TRUSTe nem volt hajlandó vizsgálatot indítani a RealNetworks ellen, mert a szabályzatuk szerint a minősített partner csupán azt vállalja, hogy a honlapján keresztül nem gyűjt információkat, s az embléma hatásköre nem terjed ki a szoftverre.

Kérdéses, hogy vajon a felhasználók számára is ennyire élesen elválik-e egy szoftverkészítő honlapja és terméke. Fogyasztói-letöltői szemmel nézve – kis túlzással – nem sokban különbözik ez attól, mintha egy szoftvertermék dobozán szerepelne egy trustmark embléma, míg a szoftver maga intenzíven megfigyelné a felhasználót.

Rendkívül fontos észrevenni, hogy a kellemetlenségeket, a problémákat a jogszerűen eljáró fogyasztók élték meg. Ez visszas helyzetet teremt annyiban, hogy a kiadók, stúdiók, szoftverkészítők egyfelől a perekkel, a tolvajnak címkézéssel, és lobbitevékenységükkel afelé terelik a fogyasztókat, hogy illegális letöltések és másolás helyett vásárolják meg a kívánt tartalmat. Másfelől a tartalmat olyan eszközökkel látják el, amelyek egyes esetekben csak „megnyomorítják” az élményt.

3.8. Összefoglalás

A DRM gazdasági megalapozottságába vetett hitet megingatja az a tény, hogy a zeneipar óriásai egymás után hagytak fel a DRM rendszerek alkalmazásával a zenei CD-ken, ráadásul a négy nagy közül az egyik már az online zeneértékesítés területéről is kivonta a digitális jogkezelő rendszereket. Emellett mégis figyelemre méltó az iTunes Music Store sikere, melynek esetében a tartalmat DRM rendszer védi. Az iTMS sikeréhez azonban nem a DRM járult hozzá, hiszen a fogyasztók számára a DRM semmilyen többletet nem nyújt, sőt, a DRM rendeltetése a fogyasztói érték csökkentése lenne, a felhasználási lehetőségek korlátozásával. Számos vásárló mégis többre értékelte a DRM-el védett, korlátozott tartalmat az ingyenes, fájlcserélő hálózatokról letölthető tartalmaknál. Racionális gondolkodást feltételezve ez a jelenség nem írható a DRM javára. A DRM-ek közvetlen gazdasági hatása a fogyasztókra a számtalan illegális forrás miatt egyelőre nem releváns. A fogyasztók nem azért választották az iTunes-t, és nem azért adtak ki számonként 1 dollárt, vagy 1 eurót, hogy DRM-el védett zenéjük lehessen. Valójában nem tudni, hogy miért volt hajlandó ez a sokaság megvásárolni ezeket a tartalmakat. A megvásárolt tartalmak tekintetében a DRM-nek nincs semmi hatása, hiszen ugyanaz a tartalom ingyen is elérhető fájlcserélő hálózatokon. Az egyetlen, amit a DRM rendszer elér, hogy korlátozza a jogszerűen eljáró fogyasztó lehetőségeit, míg a fájlcserélés jelenségét nem szorítja vissza.

A DRM valójában rossz helyen avatkozik a folyamatba, lévén a tökéletes digitális másolat létrehozását akarja megakadályozni. Fogyasztóból azonban rengeteg van, és ezek között akad olyan, aki számára a DRM rendszer feltörése kihívás, kis ferdítéssel azt is mondhatnánk, hogy számára jobb ár-érték aránnyal bír, mint a felhasználási jogok megvásárlása. És elég csak egyiküknek sikerrel járnia ahhoz, hogy a tartalom elérhetővé váljon az interneten, a feltörés módszerével együtt.

A már feltört, illetve a még töretlen DRM típusok aránya segít annak eldöntésében, hogy a DRM rendszerek, vagy a felhasználók állnak-e „nyerésre”.

5. A DRM jövője

Nem tűnik valószínűnek az, hogy a DRM rendszerek örökre eltűnjenek a tartalom előállítók piacáról, ahogy mindig lesz olyan vállalatokra is példa, akik azon közönség számára kínálnak majd termékeket, szolgáltatásokat, akik szívesen áldoznak a korlátozásoktól mentes tartalmakra. A DRM-mel telített piac gondolata legkésőbb akkor dőlt meg, amikor a négy nagy zenei kiadó elhagyta a másolásvédelmi intézkedéseket a CD lemezeiről. A DRM-től teljes mértékben mentes digitális javak piaca azért valószínűtlen, mert mindig lesznek olyan tartalmak, melyeket a tulajdonosa, vagy terjesztője nem tömeges fogyasztásra szán, hanem egy-egy vásárló számára, jellemzően magas ellenérték fejében. Tipikusan ebbe a kategóriába sorolhatóak a kutató és tanácsadó cégek által készített tanulmányok.

Jelenleg számos kezdeményezés indul új piaci szereplőktől a digitális világban való értékteremtés innovatív megvalósítására, s az ily módon létrejött tartalmak minden esetben másolhatók. A DRM rendszerek ellenben azt próbálják elérni, hogy ne legyen másolható az, ami létéből fakadóan másolható. Míg egyes tartalom-előállítók a régi üzleti modelljükért indítanak harcot a jogszabályok és a digitális védelem területén, addig más vállalatok megjelennek mellettük, és egymás után rukkolnak elő újabb és újabb lehetőségekkel. Az új üzleti modelleket kipróbáló vállalatok egy része inkább a szolgáltatásért számol fel díjat a fogyasztónak, nem az adatokért. A digitalizálható analóg termékek önmagukban egyre kevésbé jelentenek értéket, ahogy a célközönség egyre nagyobb része ismeri meg fájlcserelés lehetőségét.

A digitális tartalmak előállítói számára a lehetőségeket két csoportba lehet sorolni. Egyrészt a vállalat megpróbálhat a jelenlegi, vagyis a tömeges fájlcserelés előtti üzleti modellre építve egy speciális környezetet kialakítani a termékek számára. Úgy tűnik, hogy ez a „szigorú konzervatív” irány a jellemző a legtöbb kiadóra, stúdióra és szoftverkészítőre.

A másik lehetőség az, hogy új üzleti modelleket próbálnak ki az előállítók és a terjesztők, melyben a digitális korszak hátrányaiból próbálnak előnyt kovácsolni. Ez a „megengedő innovatív” megközelítés főleg az újabb cégekre jellemző. Nem véletlen, hiszen a zene-, film- és szoftveripar erősen centralizált, s a piacra belépni a tőkeerős vállalatok mellé nem könnyű egy kisvállalkozásnak. Ezek a cégek próbálnak ki minden olyan lehetőséget, amelyet a régi „nagyok” nem hajlandóak. A Flickr (később részletezve) vagy a YouTube példáját

megvizsgálva pedig látható, hogy a helyzet nem teljesen reménytelen. A következő alfejezetekben azt vizsgálom meg, milyen lehetőségek is állnak a „szigorú konzervatív” és a „megengedő innovatív” vállalatok előtt. Ez a kitekintés rövidtávra szól, és többnyire létező kezdeményezésekre épít.

5.1. Szigorú konzervatív

5.1.1. Erősebb kontroll

A vállalat a hagyományos üzleti modelljét védelmezve a DRM rendszerek hatékonyságát és elterjedtségét kénytelen fokozni. Az információk korlátozása és az adatok titkosítása egyre megbízhatóbb kell legyen. Ezt a célt kétféleképp lehet megközelíteni. Egyrészt a jelenlegi, csak-szoftver alapú DRM rendszerek újabb és újabb változatainak elkészítésével. Másrészt a szoftvereknél mélyebbre nyúlva, a hardvereken keresztül egy biztonságosabb alap készítésével.

Az egyik nagyszabású kezdeményezés a hardver alapú jogkezelés területén a Trusted Computing Platform Alliance (új nevén Trusted Computing Group) munkája. A csoportot többek között az AMD, HP, IBM, Microsoft, Sun Microsystems kezdeményezésével hozták létre, hogy a bizalmi számítástechnika gondolatát a gyakorlatba ültessék. (Wikipedia – Trusted Computing Group)

A bizalmi számítástechnika lényege, hogy a számítógépen a behatolási pontokat minimalizálni kell, és a számítógép érintetlenségéért ki kell nevezni felelősnek egy olyan hardver eszközt, amit csak nagyon nehezen lehet feltörni, és amíg ez nem történik meg, addig ez az eszköz felügyeli, hogy a számítógép egyes komponensei (hardver és szoftver) érintetlenek legyenek. Ezt az eszközt a gyakorlatban Fritz-chipnek nevezik, és a számítógép indulása során felügyeli azt, hogy egy biztonságos, jól ismert környezet jöjjön létre, melyben nincs nyoma kártékony változtatásoknak. Ennek alapja, hogy a számítógépben történő minden adatforgalom titkosítottan történik, és az egyes folyamatok nem férnek hozzá a másik adataihoz.

A technológia elméletileg képes arra, hogy a felhasználó biztonságban tudhassa a számítógépét kártékony programoktól, azonban a kritikusok felhívják a figyelmet arra, hogy a technológia valójában nem a felhasználó számára teszi megbízhatóvá a rendszert, hanem a tartalom előállítók számára. Az adatok titkosítása és a folyamatok felépítése lehetőséget ad

arra, hogy a tartalomtulajdonosok, szolgáltatók bármikor visszavonják a felhasználó jogait. Gyakran hozzák példaként azt, miszerint a technológia lehetővé tenné, hogy a felhasználó által készített dokumentumot elérhetetlenné tegye szövegszerkesztő szoftver írója, amennyiben a szoftver licenc lejár, vagy – szélsőséges esetben – ha a tartalom nem tetszik a cenzornak. Mivel minden adat a készítő program által titkosított, a szoftverkészítők a fogyasztókat meglehetősen egyszerűen leköthetik.

Amennyiben a kritikusoknak hinni lehet, úgy a szigorú konzervatív tartalom előállítók és szolgáltatók számára ez a megoldás mindenképp támogatandó. Jelenleg már létezik olyan törvényjavaslat Amerikában, mely kötelezővé tenné, hogy ezt a technológiát minden számítógép támogassa, és a régi, „védtelen” számítógépek ne csatlakozhassanak az internetre.

5.1.2. Új jogszabályok

Egy szigorú konzervatív vállalat számára szükséges, hogy minél szigorúbb, és kivételektől mentes jogi szabályozás szülessen, ami egyrészt támogatja a DRM rendszerek elterjesztését, biztosítja a szabályok szintjén, hogy a fogyasztók ne tehessenek ellene semmit, és alapot nyújt arra, hogy felléphessenek a non-konformista felhasználókkal szemben.

Egyelőre úgy tűnik, hogy a DRM támogatását illetően sokkal szigorúbb jogszabályokat nem lehet létrehozni, mint a jelenleg hatályosak. A DMCA és az EUCD is megtiltja a DRM rendszerek megkerülését szolgáló eszközök előállítását, forgalmazását és forgalmazásában való részvételt. Az EUCD esetében az a probléma, hogy a tagállamok eltérő módon adaptálták a saját jog-rendszerükbe, így nem nyújt Európa-szerte egységes alapot a vállalatok számára. Egyrészt ezen hézagok befoltozását támogathatná és támogatja is a szerzői jogi ipar.

Másrészről az adatvédelmi fejezetben már szó volt arról, hogy a DRM-ek jogszerű működéséhez vagy lazítani kéne a jelenlegi adatvédelmi szabályokon, vagy olyan technológiát kéne kifejleszteni, ami a felhasználók személyes adatait védve képes betartatni a tartalomhoz kapcsolódó felhasználási jogokat.

Harmadrészt szükség volna arra is, hogy a DRM rendszerek kompatibilitásával kapcsolatos kérdések megválaszolódjanak. Jelenleg is vannak olyan országok, amelyek a DRM rendszereket törvénytelennek minősítették, amiért a fogyasztók által megvásárolt tartalmat a fogyasztó nem tudja bármilyen olyan eszközön felhasználni, amely eszköztől ez elvárható volna.

5.2. Megengedő innovatív

5.2.1. Új jogi hozzáállás

A jogi hozzáállás változtatásával elejét lehetne venni az iparágban egyre népszerűbb peres eljárásoknak. A RIAA, az MPAA, és Magyarország esetében a ProArt jogvédő szervezetek tevékenysége kihat a mögöttük álló vállalatokra. Bár előfordulhat, hogy a peres esetek számának növekedését elítélő lakosok a jogvédő szervezeteket hibáztatják ezekért, a zene- és filmipar centralizáltsága miatt pontosan lehet tudni azt is, hogy kiknek az érdekében folynak a perek. Valójában a jogvédő szervezetek nem tesznek mást, mint megpróbálják a tagok törvény által biztosított jogait érvényesíteni, még ha a módszereik kifogásolhatóak is.

A jelenség megoldása jogi vonatkozásban kétféleképp oldható meg. Egyrészt a törvényi szabályozás lazításával, másrészt a szerzői jogosultak hozzáállásának változásával. Ez utóbbit támogatandó számos kezdeményezés született, amely rendkívül egyszerűvé teszi a Szerzői jogi törvény biztosította kizárólagos jogok közötti válogatást aszerint, hogy a szerző mely jogait szeretné megtartani, és melyekről mond le.

A szerzői jog által biztosított kizárólagosság egy részéről való lemondás egyre népszerűbbé válik a tartalomelőállítók körében. A Flickr internetes fotómegosztó oldalon már több, mint 400 millió képet tettek közzé felhasználók, s a Flickr honlap szerint ebből több, mint 35 millióra valamilyen Creative Commons (CC) licenc vonatkozik.

A Creative Commons licenc egy egyre népszerűbb licenc forma, melynek alapjait Lawrence Lessig hozta létre, és egyre több ország jogi szabályaihoz adaptálják, s már a magyar jogszabályokhoz alakított változat is elérhető a CC csoport honlapján. A különlegessége, hogy rendkívül egyszerűen választhatja ki a szerző, hogy milyen jogokat kíván fenntartani magának, és milyen jogokról mond le a társadalom számára. A CC alatt licencelt tartalom szabadon terjeszthető bárkinek, bármikor. A szerző azt a kikötést is megteheti, hogy művét csak nem-kereskedelmi célból használhatják fel, kereskedelmi felhasználás esetén az engedélyezés joga a szerző kezében marad. A licenc másik különlegessége, hogy a jogok nem visszavonhatók. Míg a Szerzői jogi törvény biztosítja a lehetőséget arra, hogy a szerző a művét visszavonja, és a publikálását megtiltsa, a Creative Commons licenc ezt nem engedélyezi. Amilyen licenccel a szerző közzéteszi a művet, az a licenc fog rá vonatkozni mindaddig, amíg a mű közkinccsé nem válik. Ennek oka rendkívül egyszerű. A CC licencet

direkt a digitális világ szabályainak megfelelően alkották. Az interneten egyszer közzétett tartalmat fizikailag lehetetlen onnan visszavonni, így nincs értelme annak, hogy a jog lehetőséget biztosítson valamire, ami tökéletesen ellentmond a világ szabályainak. Léteznek olyan változatok is, amelyek a Szerzői jogi kizárólagosságot biztosítják a felhasználó számára, ám az Szjt. által biztosított élettartam plusz 75 év helyett összesen 14 évre szól. Létezik olyan CC licenc is, ami a fejlett országokban a szokásos kizárólagosságot biztosítja, míg a harmadik világ országainak számára szabad hozzáférést biztosít.

A jogosultak hozzáállásának változására lenne szükség a kizárólagos jogok időtartamát illetően is. Míg az 1790-től 1970-es évekig a szerzői kizárólagosság joga harminc év körül alakult, ma már a szerző halálától számított hetven-hetvenöt év a védelem ideje.

Ilyen hosszú korlátozás teljes mértékben értelmetlen. Az a társadalmi generáció, amely közvetve hozzájárult az alkotás elkészüléséhez, jó eséllyel nem férhet hozzá szabadon, hiszen mire a védelmi idő lejár, már egy másik generáció tölti idejét a földön.[6]

5.2.2. Új üzleti modell

Az előző pontban szó volt arról, hogy szigorú jogi kizárólagosságok betartása, betartatása, és a jogok megsértésének üldözésére léteznek jogi alternatívák. Az egyre szaporodó perek és a fogyasztók csökkenő bizalma azonban nem fog változni attól, hogy lehet másként is csinálni. A szerzői jogosultak mentalitásának változására van szükség. Az új üzleti modelleket kereső vállalatok számára a berögzült jogi gyakorlattal való szakítás kitűnési lehetőséget biztosíthat, mint például a CC licenc használata a „minden jog fenntartva” helyett.

Az új utakat kereső alkotók számára a már említett CC licenc is üzleti előnyt jelenthet, bár ez első látásra nem tűnik egyértelműnek, hiszen a licenc alapja az, hogy a jogosult lemond a forintosítható jogok egy részéről. A mozgalmából mindenesetre annyi tanulság leszűrhető, hogy ha nem muszáj, akkor feleslegesen ne védjünk.

Nem csak a megengedőbb licencfeltételek vezethetik ki a társadalmat az egyre szaporodó fájlcseréi perek világából. Van olyan kezdeményezés, mely a fájlcseréi folyamatát a digitális világból az analóg világba ülteti át, és nem kevés sikerrel. A Netflix nevű amerikai cég is ezt az ötletet alkalmazza működése során. Internetes fájlcserélő rendszer üzemeltetése helyett offline fájlcseréi szolgáltatást biztosít az előfizetőinek. Havi díj ellenében az előfizető DVD-ket rendelhet meg, amelyeket korlátlan ideig magánál tarthat.

Amennyiben új DVD-kre kíváncsi, úgy a már megrendelt és kiszállított DVD-ket vissza kell küldenie a központba, hogy az új rendelését megkaphassa. Jelenleg 6,3 millió előfizetője van, akik 70 ezer film közül választhatnak. A napi rendelések száma 1,4 millió DVD. A cég 2007. február 25-én szállította ki az egymilliomodik DVD-jét.

Hasonló elven működik a Peerflix, melynek előfizetői egymással cserélnek DVD-t. Az előfizető beadja saját DVD-it a talonba, melyért cserébe kérhet DVD-ket a talonból. A La La és a PaperBackSwap cégek ugyanezt a szolgáltatást nyújtják audio CD és könyvek tekintetében.

Ez a modell nem teljes mértékben analóg a digitális fájlcserelés folyamatával, mivel a cserélgetések során a digitális megoldással szemben nem képződik automatikusan egy másolat, azaz a flix-típusú megoldások esetén valódi cseréről van szó, a másodkéz piacáról.

A termékek cseréje ezek szerint képes életben tartani vállalkozásokat. A konzervatív vállalatok azt szeretnék, ha a termékük digitális formában legfeljebb egyszer utazhatna a világhálón: a tartalomszolgáltatótól a fogyasztóig, míg a fogyasztóktól fogyasztóknak terjesztés lehetőségét minden eszközzel támadják. Létezik emellett egy harmadik út is, amikor a vállalat, vagy szerző a termékét nem adja ki a keze közül. Ez a szoftverkészítő cégek számára nyújthat megoldást a fájlcsere jelenséggel szemben. Talán legismertebb példája a modellnek a World of Warcraft nevű játék. Lényege, hogy a játékosok előfizetési díj ellenében a Blizzard cég központjában futó játék-szerverre kapcsolódhatnak, és így tudnak játszani. Hiába osztják meg a játékosok a szoftvert fájlcsereáló hálózaton, a minőségi játékhoz szükség van arra, hogy előfizessenek a cég szervereihez való hozzáférésre. Gyakorlatilag a játékszoftver fele a Blizzard cég tulajdonában marad fizikailag is, és a másik fele az, ami a boltok polcaira kerül.

Ugyanezen az elven működnek a webalapú applikációk is. A Flickr album oldala, a Google Docs, a Google Calendar lényege az, hogy a felhasználó hozzáfér a tulajdonos szervereihez, miközben a szoftver nem a felhasználó gépén fut, hanem házon belül, a vállalatnál marad. A szoftverkészítő nem egy kézzelfogható terméket, vagy tárolóeszközökön elhelyezhető bitsorozatot árul, hanem szolgáltatást.

Nyilvánvalóan nem teheti meg az összes szoftverkészítő azt, hogy az applikációt webszerverekre helyezze, és a szoftver szolgáltatásait kezdi árulni. Nem működhet ez egy operációs rendszer készítője számára, hiszen egy operációs rendszer a jelenlegi teljesítmények mellett szükséges, hogy a helyi számítógépen fusson. Mégis vannak olyan vállalatok, amelyek

nem a szoftver kalózkodás elleni harcba fektetik a pénzüket, hanem ingyen elérhetővé teszik terméküket, és az előző példában szereplő cégekhez hasonlóan csak a szolgáltatásaikat bocsátják áruba. Ezek rendszerint a operációs rendszer működtetésével kapcsolatos támogatás biztosítását jelentik, de más termék-specifikus szolgáltatás is szóba jöhet, mint például felhasználói kurzusok biztosítása. Ilyen cégekre és operációs rendszerekre bőven akad példa a Linux disztribúciók körében. Ezzel a modellel próbálja életben tartani magát a Red Hat nevű cég is. Tehát a digitális javak másolhatósága miatt egyes cégek a harc helyett új üzleti modelleket próbálnak ki, és inkább a szolgáltatásaikra fektetik a hangsúlyt. A szolgáltatás ugyan nem lehet fájlcsereelő folyamatok tárgya, azonban a szolgáltatások is lemásolhatóak. Ez azonban jóval több befektetést igényel, mint egy digitális jószág lemásolása, így a szolgáltatások klónozása főleg a vállalati szférán belül marad. Mivel a szolgáltatások általában nem levédhetők, így az egymás után megjelenő vállalatok a versenyt fokozzák, és arra készítetik a többi vállalatot, hogy szolgáltatásukat minél versenyképesebbé és innovatívabbá tegyék.

A termék-szolgáltatás dichotómia a zeneipar esetére is leképezhető. Az együttesek terméke a zeneszám, melyet CD-lemezen vagy online zeneboltban terjesztenek, és melyek fájlcsereelő hálózaton keresztül általában elérhetőek. Az együttesek által nyújtható, egyedi és nehezen másolható szolgáltatás a koncertezés. A Rolling Stones zenekar bevételeinek 92%-át a koncertjegyek adják. Ebből a stúdiók nem részesednek, így nem csoda, hogy az ingyenes zeneszámok nem üzleti érdekük. Az ingyenes zenével csak az együttesek és a fogyasztók járnak jól.

Ez nem nyújt megoldást minden szereplő számára. Például egy zeneszerző nem tudja előadni élőben a szerzeményét, és a stúdiók dolgozói sem állhatnak színpadra, hogy munkájukért cserébe fizetést kaphassanak. Ez azonban az üzleti modell hibája. Ha a zene és filmipar azt állítja, hogy a működésük a jelenlegi körülmények között nem fenntartható, akkor a probléma az üzleti modelljükben van. Ők voltak azok, akik így építették fel a vállalkozásukat. Hasonló a helyzetük a dunai komposokéhoz, akik először szembesültek azzal, hogy hidak épülnek a folyók fölé. Az üzleti modelljük azon alapult, hogy az emberek át akarnak jutni egyik partról a másikra.

Fel lehet róni az analógiának, hogy a hidak esetén hídpénzt kellett fizetni, így nem ingyenes alternatívát nyújtottak a komposokkal szemben. Azonban az sem teljesen igaz, hogy a stúdiók zeneterjesztői feladatainak alternatívája, a fájlcsere, teljesen ingyenes lenne. Ha másért nem,

hát az internet előfizetési díjak rendszeres fizetése mindenképp szükséges az amúgy ingyenes szolgáltatás igénybevételéhez. A filmipari megfelelője a koncertezésnek a filmvetítés, más szóval a mozi. A mozikban történő vetítések után kezdik a stúdiók terjeszteni a terméket lemezes változatban, és csak ezután kerül a tévék képernyőjére. Ez egy jól bevált sorrend a filmipar számára, habár belegondolva nem biztos, hogy logikus, hiszen a tévés vetítések előtt a fájlcsereklők megtelnek a DVD minőségű, ingyenesen letölthető filmmel.

A filmvetítés legnagyobb problémája szintén az üzleti modellben keresendő. Egyrészt a mozibemutatók előtt gyakran elérhető a filmek azon változata, melyet DVD minőségben a sajtó számára elérhetővé tett a stúdió. Másrészt a mozibemutatók időpontjai között földrészenként vagy országoként akkora ugrás lehet, hogy a kettő között valahol a filmet már DVD-n is kiadják, és így egyes országbeli letöltők a filmet előbb megnézhetik, mint hogy az a moziba kerülne hazájukban. Ez a fajta üzletpolitika teljes mértékben figyelmen kívül hagyja az internet hálózat globális jelenlétét, és azt, hogy digitális javak esetében a regionális szegmentáció ebben a formában értelmetlen. A filmipar jelentős javulást érhetne el azáltal, hogy az egyes termékváltozatainak időablakait ésszerűbben rendezi el, s ezzel a támadási felületek számosságát redukálhatja. Egy olyan világban, melyben a digitális termék az árucikk, valódi hasznót csak az élmény nyújthat. [2]

Végül ki kell térni az árazás kérdésére is. A Creative Commons licenc esetében volt szó arról, hogy egyes alkotók a műveik ismertsége érdekében hajlandóak lemondani kizárólagos jogaikról, hogy később valamilyen formában anyagi előnyhöz jussanak. Az ingyenes terjesztés, és anyagi előnyhöz jutás érdekes kombinációját alkalmazza az Amie Street nevű cég, melyet 2006-ban alapított néhány végzős egyetemista. Az Amie Street egy online zeneboltot üzemeltet, melyben a zeneszámok eleinte ingyen letölthetők, és egy bizonyos szintű ismertség elérése után az árak fokozatosan emelkedik, egészen 98 centig darabonként, így 1 centtel olcsóbbak az iTunes Music Store-nál is, ráadásul a letöltött zenét nem védi DRM.

Az eddig felsorolt lehetőségek, példák mind egyfajta takarékosági elvre épültek, arra, hogy miként lehet kevesebből jobban megélni. Az analóg és digitális disztribúció helyett miként működhet a Peerflix az analóg, postai cserélgetésre alapozva. A bárhol elérhető játékszoftverek helyett milyen sikerekkel kecsegtet az MMORPG-k lehetősége. A termék/szolgáltatás csomag helyett miként hagynak fel a vállalatok a termékük árazásával, s

koncentrálnak helyette csak a szolgáltatások piacára. A zeneipar számára a biztos bevételi források közül a koncertezés szerepe egyre hangsúlyosabbá válik.

Az eddigieken túl léteznek olyan vállalatok is, akik teljesen új utakat próbálnak ki. Egyik példa erre a Sellaband, mely vállalkozásnak az üzleti modellje valószínűleg az eddigiek közül a legújyszerűbb. A Sellaband oldalára bármilyen előadó feltöltheti alkotását, ahonnan az szabadon letölthetővé válik. A felhasználók pénzüikkel szavazhatnak azokra az előadókra, akikről úgy gondolják, hogy elég jók ahhoz, hogy sikerre vihessenek egy CD albumot is. Mindezt jövőbeli részesedésért teszik. Amennyiben összegyűlik ötvenezer dollár támogatás egy csoport vagy előadó számára, úgy zenéjüket profi stúdióban rögzítik, CD-jüket pedig világszerte árusítani kezdik. A bevételek fele az előadókhöz kerül, míg másik felét elosztják azon rajongók között, akik hozzájárultak az ötvenezer dolláros indulótökéhez. Mindeközben az előadó zenéje a weboldaltól továbbra is ingyen letölthető, s az oldalon elhelyezett reklámbevételekből a művész 1/3 arányban részesedik, a támogató felhasználók („hívők”) szintén megkapják a bevételek 1/3-át, és a maradékot a Sellaband kapja.

A kezdeményezés túl fiatal ahhoz, hogy hosszú távú jövőjét meg lehessen becsülni. Eddig négy olyan előadó szerepel az oldalukon, akik elérték az 50.000 dolláros küszöböt. A „hívők” befektetéseinek megtérüléséről épp ezért egyelőre nincsenek adatok. A kezdeményezés azonban mindenképp figyelemreméltó, és fel kell hívja a figyelmet arra, hogy egészen újszerű modellekben is lehet gondolkodni, nem kell megragadni a hagyományos megoldásokban.

Szintén napjainkban terjed az a látásmód, hogy a kreatív alkotók saját web-oldalukon ingyenesen teszik közzé alkotásaikat, de lehetőséget biztosítanak arra, hogy aki megteheti, és módjában áll, az támogassa az alkotót. Ezt adakozásnak, angolul contribute-nak nevezik. Ennek a rendszernek a hiányossága olyan pénzáthelyezési módszer elterjedése, melynek segítségével kisebb összegeket, olcsón lehet bankszámláról bankszámlára juttatni. Az adakozási lehetőséget fenntartó alkotók általában a PayPal donate rendszeren keresztül várják a támogatásokat. A PayPal egy hagyományos bankszámlához hasonló, saját egyenleggel rendelkezik. Azonban a megszokott 3x8 számjegy helyett itt e-mail cím alapján történik a számlák azonosítása. A PayPal rendszer nagy előnye, hogy a rendszeren belüli tranzakciók díjmentesek (a fogadó fél fizeti a tranzakciós díjat), és azok pillanatokon belül lezajlanak. A rendszer használatához dombornyomott bankkártya, vagy hitelkártya szükséges.

6. Összefoglalás

A digitális kapu feltárásával olyan lehetőségek birtokába jutottunk, melyek mindaddig elképzelhetetlenek voltak, s így nem is lehetett felkészülni az ismeretlen jelenségek fogadására. A jogi szabályozás jelentős lemaradással próbál lépést tartani a digitális világ lehetőségeivel. Egyelőre úgy tűnik, hogy a jogalkotói folyamat szembemegy a helyesnek tűnő iránnyal.

A nagyvállalatok DRM-től való visszavonulása azt a látásmódot támasztja alá, hogy nincs szükség szerzői jogkezelő rendszerekre. Véleményem szerint a fogyasztók két ellentétes irányzat között lavírozva próbálnak utat találni. Ezt az útkeresést azonban a működő DRM rendszerek nem segítik, hanem inkább akadályozzák.

A fogyasztókat egyik oldalról a tartalmak legális felhasználására ösztönzik (szerzői-jogi kampányok, stb.), a másik oldalról pedig azt próbálják megértetni velük, hogy amit megvásároltak az nem teljesen az övék, nem használhatják fel azt korlátlanul, és ha más formátumban szeretnék élvezni, akkor újra kénytelenek megvásárolni. Abban az esetben pedig, ha ezeket a szabályokat megszegik komoly büntetésre számíthatnak.

Ez az állapot hosszú távon nem tartható fent. Mégis mivel a történelem során a fejlődés iránya mindig egybeesett a gazdasági érdekekkel, jelen esetben megkockáztatom kijelenteni, hogy a DRM léte gazdasági érdekek miatt sokáig megkérdőjelezhetetlen marad.

Dolgozatomban bemutattam a jogkezeléshez vezető út legfontosabb állomásait, a DRM születésekor bábáskodó szereplőket, a leginkább elterjedt megoldásokat, azok hibáit, valamint a jelenlegi legmodernebb törekvéseket.

A bemutatott rendszerek esetében igyekeztem a legszélesebb spektrumú képet adni a megoldások technikai hátteréről, amennyiben ez lehetséges volt.

A különböző rendszerek hibáin alapuló, töréseket kihasználó alkalmazásokat kizárólag szabadon, bárki számára ingyenesen hozzáférhető forrásokból szereztem be. Annak érdekében, hogy ne legyek vádolható ezen alkalmazások terjesztésével ezeknek a programoknak a pontos forrását nem árulom el (akit igazán érdekel úgyis megtalálja őket). Dolgozatom írásakor nem „kalózkézikönyv” elkészítése volt a célom, hanem komplex tényfeltárás, mely esetenként olyan összefüggésekre is rávilágít, melyek egyébként nem lennének olyan szembeötlőek.

7. Irodalomjegyzék

1. Adobe (2007): Adobe to Release PDF for Industry Standardization
<http://www.adobe.com/aboutadobe/pressroom/pressreleases/200701/012907OpenPDFAIIM.html>
utolsó letöltés: 2008. február 29.
2. Andersen, C. (2007): Give away the music and sell the show
http://www.longtail.com/the_long_tail/2007/01/give_away_the_m.html
utolsó letöltés: 2008. február 29.
3. Bangeman, E. (2004): Apple responds to RealNetworks FairPlay hack. Arstechnica
<http://arstechnica.com/news.ars/post/20040729-4051.html>
utolsó letöltés: 2008. február 29.
4. BBC (2007): Hi-def DVD security is bypassed
<http://news.bbc.co.uk/2/hi/technology/6301301.stm>
utolsó letöltés: 2008. február 29.
5. Bell, D. (2006): Settec Alpha-DVD protection used on German Mr.& Mrs.Smith
http://www.cdfreaks.com/news/Settec-Alpha-DVD-protection-used-on-German-Mr_-Mrs_Smith.html
utolsó letöltés: 2008. február 29.
6. Bodó Balázs (2006): Mi a Creative Commons? Amit kihoznak belőle... . IT.News
http://itcafe.hu/cikk/mi_a_creative_commons_amit_kihoznak_belole/mi_a_creative_commons.html
utolsó letöltés: 2008. március 01.
7. Borland, J. (2004)a: Judge slows MPAA file-trading suits. CNET News
http://news.com.com/Judge+slows+MPAA+file-trading+suits/2100-1025_3-5466215.html?part=rss&tag=5466215&subj=news.1025.20
utolsó letöltés: 2008. március 01.
8. Borland, J. (2004)b: RIAA hits minor swap suit setback. CNET News
http://news.com.com/RIAA+hits+minor+swap+suit+setback/2110-1027_3-5171959.html
utolsó letöltés: 2008. március 01.
9. BSA (2006): Új lendülettel folytatódik a BSA Nagyvizit kampánya
<http://www.bsa.org/hungary/press/newsreleases/BSA-Nagyvizit-kampany.cfm>
utolsó letöltés: 2008. március 01.
10. Chai, W. (2005): Microsoft halves Windows prices in China. ZDNet Asia
<http://www.zdnetasia.com/news/software/0,39044164,39219592,00.htm>
utolsó letöltés: 2008. március 01.
11. Cohen, J. (2003): DRM and Privacy. Berkeley Technology Law Journal
<https://www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.html>
utolsó letöltés: 2008. március 01.
12. Gasser, U. (2006): EUCD Best Practice Guide Released
<http://blogs.law.harvard.edu/ugasser/2006/12/07/eucd-best-practice-guide-released/>
utolsó letöltés: 2008. március 01.
13. Graves, L. (2004): Has TiVo Forsaken Us?. Wired
<http://www.wired.com/wired/archive/12.11/view.html?pg=3>
utolsó letöltés: 2008. március 01.

14. Groenenboom, M. (2005): Comparing the EUCD implementation of various Member States.
INDICARE
http://www.indicare.org/tiki-read_article.php?articleId=88
utolsó letöltés: 2008. március 02.
15. HBO: FAQ
<http://www.hbo.com/corpinfo/cgmsafaq.shtml>
utolsó letöltés: 2008. március 01.
16. IIPA (2007): 2007 Special 301 Report HUNGARY
<http://www.iipa.com/rbc/2007/2007SPEC301HUNGARY.pdf>
utolsó letöltés: 2008. március 02.
17. Lessig, L. (2005): Szabad kultúra. Kiskapu
ISBN: 963 9637 00 9
http://www.szabadkultura.hu/htmlkonyv/free_culture.html
18. Microsoft: Benefits of Windows Media DRM
<http://www.microsoft.com/windows/windowsmedia/forpros/drm/benefits.aspx>
utolsó letöltés: 2008. március 01.
19. Wikipedia: 2005 Sony BMG CD copy protection scandal
http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal
utolsó letöltés: 2008. március 02.
20. Wikipedia: Advanced Access Content System
http://en.wikipedia.org/wiki/Advanced_Access_Content_System
utolsó letöltés: 2008. március 02.
21. Wikipedia: Blu-ray Disc
<http://en.wikipedia.org/wiki/Blu-ray>
utolsó letöltés: 2008. február 27.
22. Wikipedia: Digital Millenium Copyright Act
<http://en.wikipedia.org/wiki/DMCA>
utolsó letöltés: 2008. február 27.
23. Wikipedia: Digital Transition Content Security Act
http://en.wikipedia.org/wiki/Digital_Transition_Content_Security_Act
utolsó letöltés: 2008. február 29.
24. Wikipedia: DRM
http://en.wikipedia.org/wiki/Digital_Rights_Management
utolsó letöltés: 2008. február 11.
25. Wikipedia: History of patent law
http://en.wikipedia.org/wiki/History_of_patent_law
utolsó letöltés: 2008. február 29..
26. Wikipedia: History of copyright law
http://en.wikipedia.org/wiki/History_of_copyright_law
utolsó letöltés: 2008. február 27.
27. Wikipedia: History of radio
http://en.wikipedia.org/wiki/History_of_radio
utolsó letöltés: 2008. február 29.
28. Wikipedia: iTunes Store

- <http://en.wikipedia.org/wiki/Itms>
utolsó letöltés: 2008. február 29.
29. Wikipedia: Jon Lech Johansen
http://en.wikipedia.org/wiki/Jon_Lech_Johansen
utolsó letöltés: 2008. február 29.
30. Wikipedia: List of countries by GDP (PPP) per capita
http://en.wikipedia.org/wiki/List_of_countries_by_GDP_%28PPP%29_per_capita
utolsó letöltés: 2008. február 29.
31. Wikipedia: Macrovision
<http://en.wikipedia.org/wiki/Macrovision>
utolsó letöltés: 2008. február 29.
32. Wikipedia: Portable Document Format
<http://en.wikipedia.org/wiki/PDF>
utolsó letöltés: 2008. március 02.
33. Wikipedia: RIAA
<http://en.wikipedia.org/wiki/RIAA>
utolsó letöltés: 2008. március 02.
34. Wikipedia: Sony Corp. of America v. Universal City Studios, Inc.
http://en.wikipedia.org/wiki/Sony_Corp._v._Universal_City_Studios
utolsó letöltés: 2008. március 02..
35. Wikipedia: Trusted Computing Group
http://en.wikipedia.org/wiki/Trusted_Computing_Platform_Alliance
utolsó letöltés: 2008. március 01.
36. Wikipedia: TiVo
<http://en.wikipedia.org/wiki/TiVo>
utolsó letöltés: 2008. március 02.
36. Wikipedia: XOR (Exclusive OR)
<http://en.wikipedia.org/wiki/Xor>
utolsó letöltés: 2008. március 10.
37. O'Reilly, 2002 : J2ME in a Nutshell
ISBN: 9780596002534