10.17625/NKE.2013.005

NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

ILLÉSI ZSOLT

INFORMÁCIÓTECHNOLÓGIAI KÖRNYEZETBEN ELKÖVETETT TÁMADÁSOK ÉS BŰNCSELEKMÉNYEK KRIMINÁLTECHNIKAI VIZSGÁLATA

Doktori (PhD) Értekezés

Témavezető:
Prof. Dr. Kovács László
alezredes, egyetemi tanár

2012. BUDAPEST

Tartalomjegyzék

BEVEZETÉS

Számítógépek vesznek körül bennünket. A háztartási gépek, a szórakoztató elektronikai eszközök, a mobiltelefon, az internet már szerves részei a hétköznapi emberek mindennapjainak. Az információtechnológiát – megjelenésével szinte egy időben – a felhasználók a tudományos felhasználás mellett magán- és üzleti célokra is elkezdték használni. Az új technológiák részben megfeleltetek a korábbi technológiáknak[1], így analóg módon alkalmazni lehetett a hagyományos üzleti és jogi megközelítést. Esetenként az új technológiával együtt új, vagy a korábbitól jelentős mértékben eltérő megoldások születtek[2], amelyek utat nyitottak teljesen új üzleti modellek előtt, illetve szabályozatlanságuk okán bizonytalanságot okoztak a használók köreiben.

Értekezésemben az informatikai védelem egyik speciális alágával kívánok foglalkozni: az informatikai rendszerekben keletkező nyomokkal és ezeknek az elemzésével. Az informatikai védelem az informatikai rendszerben tárolt, kezelt, rendszerezett és továbbított adatot (információt), az informatikai szolgáltatásokat, az ezeket biztosító informatikai rendszereket fenyegető tényezők elleni, az informatikai biztonság (mint megkívánt állapot) megteremtésére és fenntartására irányuló humán, technikai – környezeti, fizikai, logikai – és jogi védelmi intézkedések összessége. [1] [2 p. 6]

A védelmi intézkedések, más néven kontrollok célja tehát az, hogy az informatikai rendszer fenyegetettségét a támadások, bűncselekmények, vagy egyéb nem kívánt események valószínűségének vagy hatásának mérséklésével a kívánatos szintre csökkentse, ezáltal az informatikai biztonságot a megkívánt szinten tartsa. [3 p. 48] A fenyegetések bekövetkezésének függvényében a kontrollokat a következőképpen lehet osztályozni:

- **megelőző kontrollok**, amelyek a fenyegetések bekövetkezésének valószínűségét, vagy a nemkívánatos események által okozott károk hatását csökkentik, még mielőtt bekövetkezhetnének[3];
- **felfedező kontrollok**, amelyek a nem kívánt eseményeket azok bekövetkezte közben észlelik, és ezáltal csökkentik a kárt[4];

[1] Szerzői és szomszédos jogok, levél → e-mail; hagyományos → internetes reklám és marketing.

[2] Ilyen új technológiai megoldás például a digitális aláírás vagy az elektronikus fizetés.

[3] Ilyen kontroll például a többfaktoros authentikáció, ami csökkenti az illetéktelen behatolás valószínűségét, vagy a rendszeres mentés, ami csökkenti egy adatvesztés hatását.

- **javító kontrollok**, a melyek az eseményeket követően avatkoznak be, ezáltal csökkentve a közvetlen, vagy a későbbiekben esetleg felmerülő károkat[5]. [3] [4]

A fentiek alapján megállapítható, hogy az információtechnológiai környezetben elkövetett támadások és bűncselekmények tekintetében a rendszerekben keletkezett adatok vizsgálata az informatikai védelem része, egy olyan detektív kontroll, amely lehetővé teszi a támadások vagy jogsértések kivizsgálását, segíti az eredményes és hatékony felderítést, továbbá alapot szolgáltat a jogorvoslathoz. [5]

Értekezésem középpontjában a büntetőeljárás, pontosabban a krimináltechnika bűnügyi tudományok egyik alága áll, amely a központjában a bizonyítékokkal kapcsolatos vizsgálatok állnak. A büntetőjogi gyakorlat mellett a bizonyítékokkal, a bizonyítással kapcsolatban a polgári jog sajátos követelményeit is megvizsgálom, tekintettel arra, hogy a büntetőeljárás során is van lehetőség a polgári jogi igény érvényesítésére. Azonban e két jogág bizonyítással kapcsolatos „világképe" olyan eltéréseket mutat, amelyeket figyelembe kell venni a krimináltechnikai vizsgálatok megtervezése és elvégzése során.

Ahogy például a biológia módszerei és eszközrendszere általánosan alkalmazható bármilyen személy DNS-ének analizálására, a minta alapján a mintaadó azonosítására – függetlenül attól, hogy egy bűncselekmény vagy egy katonai akció során gyűjtötték-e be azt –, úgy az információtechnológiai eszközök és rendszerek vizsgálata során módszerek és technikák szintjén is közömbös az elkövető személye és motivációja. Krimináltechnikai perspektívából az információtechnológiai eszközöket, rendszereket ért támadások természetüket tekintve megegyeznek – függetlenül attól, hogy a támadást egy állam vagy annak egy katonai/hekker alakulata, egy politikailag motivált szervezet[6], terrorista csoport vagy egyéni elkövető hajtja végre katonai, politikai, haszonszerzési vagy egyéb céllal.

Értekezésem középpontjában informatikai igazságügyi szakértői vizsgálatok állnak. Azonban Magyarországon az igazságügyi szakértők szerepköre tág, valamennyi olyan szakkérdéssel foglalkoznak, aminek a megítéléséhez speciális szakértelem kell. Az informatikai igazságügyi szakértő tehát büntető és polgári ügyekben vizsgálhatja az infor-

[4] Ilyen kontrollok például a hálózat vagy hoszt alapú behatolás-érzékelő rendszerek, vagy az eseményt követő kivizsgálások támogatásával a felelősségre vonás vagy kártérítés során játszanak szerepet a kárcsökkentésben (pl. naplózás).

[5] Ilyen kontrollok például a hibajavító kódok, katasztrófa-elhárítási tervek.

[6] Például az Anonymus csoport.

matikai rendszerek tervezési, szervezési és üzemeltetési kérdéseit, adatbázis-struktúrákat, stúdió és multimédia körébe tartozó szakkérdéseket, berendezéseket, biztonsági kérdéseket. A tárgykör szűkítése érdekében, illetve azért, hogy a témát a Katonai Műszaki Doktori Iskola témáihoz igazítsam, az értekezésemet az információtechnológiai környezetben elkövetett támadások és bűncselekmények krimináltechnikai vizsgálatára, ezek alanyainak megismerésére, a bizonyítás és a bizonyíték fogalmának feltárására korlátozom.

Tudományos probléma megfogalmazása

Békeidőben elkövetett támadások és bűncselekmények szankcionálása a korszerű jogállamokban állami privilégium. A felelősségre vonás szabályait a jog rögzíti. Büntetés kiszabására csak törvényben meghatározott feltételek fennállása esetén van lehetőség, ugyancsak törvényben meghatározott formák és alakiság betartásával. Bíróság feladata annak eldöntése, hogy a törvényben megszabott feltételek teljesülnek-e, illetve a bíróság feladata az eljárási szabályok betartása és betartatása. [6] [7]

Tehát azok a személyek és szervezetek, akiket megtámadtak, vagy valamilyen bűncselekmény áldozataivá váltak, nem vehetik saját kézbe a megtorlást, csak bíróság útján érvényesíthetik jogaikat. Az információtechnológia elterjedésével párhuzamosan nő az ezzel kapcsolatos tényállási elemeket is tartalmazó jogesetek száma. Tapasztalataim alapján azonban a megtámadott (célpont, sértett) sokszor nem, vagy csak korlátozottan tudja a jogait eredményesen érvényesíteni. A sikeres jogorvoslat, kompenzáció gátja lehet a nem-megfelelő[7] megközelítés, amelynek következményeként:

a) nem gyűlik össze elegendő mennyiségű és/vagy minőségű bizonyíték,
b) nem készül megfelelő dokumentáció a törvényszéki vizsgálatokról,
c) a nyomkezelés nem megfelelősége miatt a vizsgálat nem megismételhető,
d) hibák keletkeznek az elemzés vagy az értelmezés során.

Értekezésem középpontjában az informatikai igazságügyi szakértés áll. Ez egy olyan **interdiszciplináris terület**, ahol a funkcionális specifikáció alapja a jog, a megvalósítás keretét a kriminalisztika adja, de az információtechnológia területén kell ezeket imple-

[7] Azaz, ha az elvégzett nyomozati tevékenység nem krimináltechnikai alaposságú.

mentálni. Az értekezésem – interdiszciplináris jellege ellenére – alapvetően informatikai mérnöki dolgozat, amely elsősorban a Katonai Műszaki Doktori Iskola sajátosságainak kíván eleget tenni.

Az információtechnológiából kinyerhető nyomok, a nyomok megszerzésének módszerei és eszközrendszere, illetve az ehhez kapcsolódó tevékenységek szempontjai azonban **eltérnek a fizikai nyom fogalma köré épített, jelenleg alkalmazott kriminálmtechnikától**. Az alkalmazott definíciók megszabják a bizonyítékok megszerzésének, rögzítésének és tárolásának a módját, meghatározzák az elvégezhető vizsgálatok körét, és értelmezési keretet biztosítanak az eredményeknek. Az anyagmaradvány és lenyomat, mint definíció jó szolgálatot tesz a fizikai entitásokból álló világ leírására. Itt mindennek vannak egyedi jellemzői, azonban az adatok egy időben több helyen is rendelkezésre állhatnak.[8] A fizikai nyom fogalma meghatározza, hogy a nyom melyik sajátosságának[9] megőrzése, feldolgozása vagy értelmezése áll a nyomozás vagy elemzés központjában. A felhasznált módszerek és eszközök a kiválasztott sajátosságnak megfelelőek lesznek. **Az informatikai igazságügyi szakértésben** éppen ezért **szükséges egy, az adat sajátosságaihoz igazodó nyom fogalmának meghatározása, amelyből kiindulva épül fel a vonatkozó kriminalisztikai nyomkezelés, feldolgozás és értelmezés**.

A gyakorlat kikényszerítette, hogy az informatikával foglalkozó szakértők kimunkáljanak olyan pragmatikus bizonyítással kapcsolatos technikákat, amelyek kiállják a tárgyalóterem próbáját. **A jelenleg alkalmazott technikák és módszertanok azonban eszköz és technológia specifikusak.** Külön-külön van módszertan a Windows, Linux, iOS és egyéb operációs rendszerekhez, a különböző fájlrendszerekhez, a vezetékes és vezeték nélküli számítógép-hálózatokhoz, mobiltelefonokhoz stb. Ezek a módszerek, technikák és eszközök nem állnak össze egységes rendszerré, nincs olyan vezérfonal, amely alapján egyértelműen eldönthető lenne ezeknek a vizsgálatoknak a kapcsolatrendszere, a szükséges szakmai kompetencia. Ennek következtében a hazai jogban alkalmazott informatikai igazságügyi szakterületi kompetenciák informatikusként nem, vagy csak nagyon nehezen értelmezhetőek[10]. Megfelelően feltárt informatikai igazságügyi módszerek és technikák hiányában a szakértőnek felteendő kérdések sem fogalmazhatók meg egyértelműen, ami-

[8] A digitálisan aláírt elektronikus dokumentumok eredetinek és hitelesnek számítanak „bitek" formájában, függetlenül attól, hogy milyen adathordozóra mikor mentették el azokat.

[9] Alaktani/lenyomat jelleg, kémiai/anyagmaradvány jelleg, esetleg mindkettő.

[10] A jelenlegi informatikai szakértői szakterületi lista alapján például nem állapítható meg egyértelműen, hogy mely kompetenciaterülethez tartozik a „fájlok keresése" feladat.

nek a következtében sokszor elbeszélnek egymás mellett a szakértők és a kirendelő hatóságok. Következésképpen **kidolgozandó egy olyan modell, amely figyelembe veszi az adat nyom-sajátosságait, rendszerbe foglalja az informatikai szakértés során elvégzendő tevékenységeket, ezek kapcsolatát, illetve támpontot ad az egyes tevékenységek elvégzéséhez szükséges szakmai kompetenciákra**.

A digitális nyom fogalmi rendszerén túl **problémát jelent** az elméletnek a gyakorlatba való átültetése, azaz, **az információtechnológiai elemet is tartalmazó helyszínek hatékony és eredményes felderítése, a nyomok biztosítása és rögzítése**. Az eljáró hatóság a helyszíni cselekményeket végző tagjainak az egyéni felkészültségétől, informatikai ismereteitől függ az, hogy mennyire lesz szakszerű, teljes körű az informatikai vonatkozású nyomokkal kapcsolatos tevékenysége. Pedig ez a feladat kiemelkedően fontos az informatikai igazságügyi szakértői vizsgálatok szempontjából. Ahogy jó minőségű és elegendő mennyiségű anyag nélkül az úri szabó sem tud jó öltönyt készíteni, úgy a szakértő sem tud hiányos adatok, rosszul rögzített nyomok alapján adekvát bizonyítékot szolgáltatni. Ezért **szükséges egy olyan egységes modell kidolgozása, amely integrálja a fizikai és az információtechnológiai sajátosságokat magában foglaló eljárásokkal kapcsolatos főbb kriminalisztikai kérdéseket**, hogy megalapozza a megfelelő protokoll és módszertani levél megalkotását.

Kutatási célkitűzéseim

Kutatásom során az alábbi részcélokat határoztam meg[11]:

Célom az **információtechnológiai környezetben elkövetett támadások, illetve bűncselekmények krimináltechnikai szempontú elemzése**; azaz, annak meghatározása,

[11] Az információtechnológiai környezetben elkövetett támadások, bűncselekmények kriminalisztikai elemzése több tudományterületet is érint, de értekezésem a krimináltechnikai feladatokra fókuszálva készült. Az informatika és a kriminalisztika általános kapcsolatával nem foglalkozom, nem kutatom a kriminálinformatika alkalmazásának lehetőségeit sem.

Értekezésemben a Unified Modeling Language (a továbbiakban: UML) technikáival modelleztem a büntetőeljárást és az informatikai (igazságügyi) szakértést. Természetesen nem célom az UML ismertetése. Mivel ez az informatikában általánosan elterjedt műszaki ábrázolás, ezért az egyes modelleknél csak speciális esetben magyarázom a modellelemeket, illetve emelem ki az értekezésem szempontjából releváns részleteket. A modellezési példáimban UML osztálydiagramokat, állapotdiagramokat és használói esetdiagramokat alkalmaztam.

Kutatási céljaimat a vonatkozó informatikai és iparági legjobb gyakorlatok felhasználásával, a technológia és hazai büntető eljárásjog összehangolásával szeretném elérni.

hogy milyen személyekről, milyen technikai komponensekből és milyen magatartásformákkal kapcsolatban lehet információtechnológiai forrású bizonyítékokat szerezni.
Kutatásom során vizsgálni kívánom, hogy az információtechnológiai rendszer, mint bizonyítékforrás rendelkezik-e olyan sajátosságokkal, amellyel az általános kriminalisztikai nyomforrások nem, ezért **rendszerezni kívánom az információtechnológia, mint bizonyíték és bizonyítékforrás sajátosságait, továbbá meg kívánom határozni a digitális bizonyítékok taxonómiáját**.

Célom továbbá **egy olyan információtechnológiai krimináltechnikai vizsgálati modell megalkotása, mely egységesíti a** jelenleg hardver és szoftver technológiák alapján **széttagolt forenzikus tevékenységeket**, integrálva az egy osztályba sorolható tevékenységek besorolási kritériumait, az egy feladatosztályba tartozó funkciókat, továbbá meghatározza az elvégzéshez szükséges szakmai kompetenciát.

Végül, de nem utolsó sorban egy olyan **magas szintű[12] modellrendszert szeretnék kidolgozni, amely egységes alapokon szemlélteti a büntetőeljárást, a szakértői szerepeket, az általános és az információtechnológiai rendszerek krimináltechnikai vizsgálatának rétegmodelljéhez igazodó főbb kriminalisztikai tevékenységeket**. Célom az, hogy ez a rendszer alapjául szolgálhasson a vonatkozó szakmai protokollnak és informatikai igazságügyi szakértői módszertani levélnek.

[12] **Magas szintű** (high-level) modell alatt olyan modellt értek, ami az információtechnológiai elemet is magában foglaló helyszíneken végzett tevékenységeket ábrázolja, a feladat egészére, a főbb funkciók és azok kapcsolatainak leírására fókuszálva.

A szakértői módszertani levelek kidolgozásának a végcélja ezzel szemben **alacsony szintű** (low level) protokoll elkészítése, ami az általános feladatoknak a részfeladatokra, funkcióegységekre történő lebontását, az elvégzendő probléma és eszköz specifikus tevékenységeket és módszereket tartalmazza. Egy-egy tudományosan megalapozott módszertani levél (alacsony szintű protokollrészlet) önálló értekezésként is megállná a helyét, ezért értekezésemben a teljes információtechnológiát feldolgozó alacsony szintű protokoll kidolgozásra hely, idő és erőforrás szűkében egyébként sem vállalkozhatnék.

Kutatási hipotéziseim

Értekezésem megírásakor abból az alapfeltevésből indultam ki, hogy az információtechnológia kriminálltechnikai vizsgálatával kapcsolatban eddig Magyarországon nem, vagy csak egyes részterületekre vonatkozóan folyt vagy folyik kutatás. Feltételeztem, hogy a kriminalisztikai vizsgálatok központi eleme a fizikai világ, azonban úgy vélem, hogy a virtuális[13] nyomok sajátos megközelítést kívánnak a törvényszéki vizsgálatok során. Ezeknek a sajátosságoknak a következményei meghatározóak a helyszíni és a laborban végzett tevékenységekkel, hardver és szoftver eszközökkel kapcsolatban. Álláspontom szerint megalkotható egy, a digitális nyommal kapcsolatos taxonómia, amely összhangban van a jelenlegi kriminalisztikai nyom fogalmával, és támpontot szolgáltat az alkalmazandó módszerekkel és technikákkal kapcsolatban.

Az eddigi informatikai igazságügyi szakértői tapasztalataim alapján úgy vélem, hogy a hazai hatóságok – kellő metodikai háttér hiányában – nem, vagy csak korlátok mellett tudják meghatározni azokat a kérdéseket, amelyekre az informatikai szakértés adhat választ. Ezt a bizonytalanságot csak erősíti, hogy a jelenlegi igazságügyi szakterületek az informatika terén nincsenek összhangban az elvégzendő feladatokkal. Még az informatikusoknak is problémát jelent a jelenlegi nómenklatúra alapján meghatározni, hogy egy-egy feladat elvégzéséhez milyen területről kérjenek fel szakértőket. Hipotézisem az, hogy meg lehet határozni egy olyan keretrendszert, amely alkalmas az informatikai igazságügyi tevékenységek, az ezek közötti kapcsolatok, illetve az elvégzésükhöz szükséges kompetenciák egységes szemléletű rendszerezésére.

Feltételezem, hogy a megtámadott szervezetek, vagy a bűncselekményeket vizsgáló hatóságok munkatársai a bizonyítékszerzésre irányuló helyszíni cselekményeknél a fizikai világra koncentrálnak[14].

Többször tapasztaltam azt, hogy a hatóságok nem gyűjtöttek össze, nem foglaltak le minden információtechnológiai szempontból releváns eszközt[15]. A praxisomban arra is

---

[13] Azaz: információtechnológiai rendszerekben előállított, továbbított, tárolt.

[14] Ezt a hipotézist megerősíti, hogy igazságügyi szakértőként rendszeresen kapok „1 db barna számítógép”-et: bűnjel-azonosító nélküli információtechnológiai eszközöket, adathordozókat.

[15] Hiányos nyomrögzítés következtében csupán a vizsgálat során derül ki, hogy csak annak marad nyoma például egy számítógép merevlemezén (azon valamikor az ügy szempontjából releváns fájllal), amit bizonyíthatóan lementettek egy ismert azonosítójú kivehető adathordozóra (USB pendrive), de a fájl már nem található meg a lefoglalt adathordozón. A mentésre használt adathordozót azonban nem foglalták le, így annak a tartalma nem vizsgálható, nem segíthette a nyomozati munkát.

volt példa, hogy az ügyben eljáró szakértők eltérő szakmai felkészültség és gyakorlat miatt eltérően értékelték ugyanazon adatokat. Véleményem szerint kidolgozható egy olyan modellrendszer, amely segít egy egységes szemléletű protokoll és igazságügyi szakértői módszertani levél kialakításában. A szabványosított módszertani megközelítés eredményeként a hatóság laikus[16] és informatikus végzettségű munkatársai, valamint az informatikai szakértők együttműködése várhatóan hatékonyabb és eredményesebb lesz. Az integrált modell segítheti, hogy a hatóság munkatársai és az informatikai szakértők közösen a lehető legtöbb – az ügy szempontjából releváns – bizonyítékot tudjanak feltárni, annak épségét megőrizni, az adattartalmat rögzíteni és helyesen értékelni.

A kutatásaim során alkalmazott módszerek

A kutatásaim során gyakorlati tapasztalataimból kiindulva széleskörű hazai és nemzetközi irodalomkutatást végeztem, hogy azonosítani tudjam a téma szempontjából leglényegesebb jogi, általános és információtechnológia-specifikus kriminalisztikai és információtechnológiai szempontokat. A megszerzett ismereteimet gyakorló igazságügyi szakértőként büntető és polgári eljárás során folyamatosan teszteltem. Az Igazságügyi Szakértői Kamarán belül – a kutatásaimra alapozva – kezdeményeztem a vonatkozó szakmai módszertani levelek kidolgozását, illetve újraélesztettem a Kamara informatikai szakértőinek szakmai konferenciáját, amelyet a jövőben szeretnék rendszeres eseménnyé tenni.

Rendszeresen részt vettem – hallgatóként vagy előadóként – a témával kapcsolatos hazai és nemzetközi tudományos konferenciákon és egyéb rendezvényeken. Kutatási eredményeimet számos tudományos konferencián ismertettem mind itthon, mind külföldön, magyar, illetve angol nyelven. Eredményeimet nemcsak konferenciákon, hanem lektorált folyóiratokban is publikáltam.

[16] Informatikai végzettséggel nem rendelkező.

Mindezek alapján dolgozatomat a következő szerkezetben építem fel:

- **1. fejezet:** Áttekintem az információtechnológiai környezetben elkövethető támadásokat és bűncselekményeket, a számonkérhetőséget megalapozó bizonyítási kérdéseket és a bizonyítékkal kapcsolatos követelményeket. Ebben a fejezetben definiálom a fizikai nyom fogalmával összhangban a digitális nyom fogalmát, megállapítva keletkezésének és jogi osztályozásának jellemzőit. Meghatározom továbbá az információtechnológiai környezetnek a krimináltechnikai sajátosságait.
- **2. fejezet:** Javaslatot teszek Brian Carrier absztrakt réteg-megközelítési modelljének továbbfejlesztésére és kiegészítésére. Így rendelkezésre állhat az informatikai igazságügyi szakértéshez egy olyan komplex taxonómia, ami alkalmas valamennyi információtechnológiai vizsgálat rendszerezésére és leírására, továbbá a szükséges kompetenciák megállapítására.
- **3. fejezet:** Elemzem az információtechnológiai környezetben végzett nyomfelkutatás, -biztosítás és -rögzítés szakszerűségének kérdéseit. Bizonyítom, hogy az információtechnológiához kötött szakértés modellezhető, és ennek a modellnek az alapján kidolgozhatóak az igazságügyi szakértői módszertani levelek. Egyúttal a fejezetben elkészítem az információtechnológiai környezetben végzett nyomfelkutatás, -biztosítás és -rögzítés magas szintű modelljét.
- Az értekezésem végén összegzem a kutatásaim eredményeit, összefoglalom azokat az eredményeket, amelyeket kutatómunkám alapján új tudományos eredménynek tekintek, illetve megfogalmazom a dolgozatom felhasználásával kapcsolatos ajánlásaimat.

I. TÁMADÁSOK ÉS BŰNCSELEKMÉNYEK KRIMINÁLTECHNIKAI VIZSGÁLATA INFORMÁCIÓTECHNOLÓGIAI KÖRNYEZETBEN

Az internetben rejlő lehetőséget nemcsak a legális üzleti vállalkozások, hanem az alvilág és a terrorista csoportok is felismerték, és egyre nagyobb jártassággal kezelik a XXI. század technológiáját – például hogy egymással kommunikáljanak, megtervezzék és összehangolják az akcióikat, pénzt gyűjtsenek, toborozzanak. [8] [9] [10] [11]

A „polgári jellegű" felhasználás mellett megjelentek az első csírái a „katonai jellegű" támadásoknak is, amit a 2007-es észt–orosz konfliktus is jól példáz. A szakirodalom egyre inkább figyelmeztet a kritikus infrastruktúrát fenyegető támadásokra, ami kivitelezhető például az azokat menedzselő/irányító számítógépekre sújtó csapással. [12] [13] [14] A magánszemélyek, üzleti vállalkozások mellett a technológia segítségével radikális politikai szervezetek, terroristák, illetve bűnözők is növelhetik akcióik, támadásaik hatékonyságát és eredményességét, valamint a technológia segíthet a nyomaik eltüntetésében is. [15] [16]

A szervezett gazdasági bűnözés mellett a kibertérben megjelentek a jellemzően 12-18 éves korcsoportba tartozó, unalomból, diákcsínyként, gondatlanságból, esetleg haszonszerzésből bűncselekményeket elkövető magányos vagy csoportokba tömörülő fiatalkorú bűnözők is. [17]

Az egyes országok eltérő szemlélete, joggyakorlata jelentős különbségekhez vezetett. Így például egy nőről készült fürdőruhás kép lehet normális családi emlék – de egyes iszlám államokban szabálysértés vagy bűncselekmény. A titkosítás használata egyes országokban alapjog, máshol hatósági engedélyhez kötött, vagy éppen tiltott. [18]

A technológia fejlődésével tehát az egyes országok – a jognak a változásokat követő természeténél fogva – egyre inkább szabályozták az információtechnológia használatát, a követendő és a jog által tiltott magatartásformákat. A jogi szabályozást követően a mindennapok szintjén is megjelentek a büntető és polgári jogsértésekkel kapcsolatos eljárások. [19]

A támadások fejlődésével a védelem is egyre nagyobb szerephez jut, a technikai-szervezési intézkedések egyre gyakrabban kerülnek előtérbe. [20] Kevés szó esik azonban a sikeres támadásokról, mivel az érintettek sokszor a jó hírnevük védelme érdekében nem is hozzák nyilvánosságra, hogy milyen támadások érték őket, és milyen károkat szenvedtek el ezek miatt. A sikeres támadások mellett még kevesebb szó esik arról, hogy

milyen módon lehet ezeket vizsgálni, hogyan lehet az elkövetőt büntetőjogi vagy polgári jogi felelősségre vonni, és a károsultak számára jogi elégtételt szerezni.

A megtámadott vagy sértett személyek, vagy szervezetek a jogsértések következményeinek felszámolására, a kártalanításért, vagy éppen a felelősségre vonás érdekében bíróságon akarnak érvényt szerezni a jogaiknak. Az eredményes és hatékony jogérvényesítéshez azonban szükség van megfelelő bizonyítékokkal alátámasztott keresetre, illetve vádra, továbbá adekvát felkészültségre, de nemcsak jogi, hanem informatikai szakterületen is. Hiszen a speciális – az információtechnológiával kapcsolatos – ügyekben a bírónak, az ügyésznek, az eljáró hatóságoknak, az üzleti/vezetői döntések meghozataláért, valamint a vonatkozó szerződések megkötéséért felelős menedzsereknek a saját kompetenciájukon kívüli területre kell merészkedniük. [21] [22] Az információtechnológiai környezetben elkövetett támadások és bűncselekmények felderítéséhez kapcsolódó speciális szaktudás az informatikai igazságügyi szakértés, az információtechnológiai bűnügyi tudomány[17] komoly segítséget adhat: segíthet a büntető vagy polgári ügyekben adekvát bizonyítékot gyűjteni és értelmezni. [23]

Az információtechnológiai környezetben elkövetett támadások és bűncselekmények krimináltechnikai vizsgálatának megfelelő megalapozásához a következőkben áttekintem ezen vizsgálatok tárgyát és alanyait, a bizonyítás és a bizonyíték fogalmát.

I.1 Támadások és bűncselekmények információtechnológiai környezetben

Értekezésem szempontjából lényeges, hogy meghatározzam azokat a magatartási formákat, melyek következményeinek és nyomainak elemzésével a támadások és bűncselekmények vizsgálatakor informatikai igazságügyi szakértőként foglalkoznom kell.

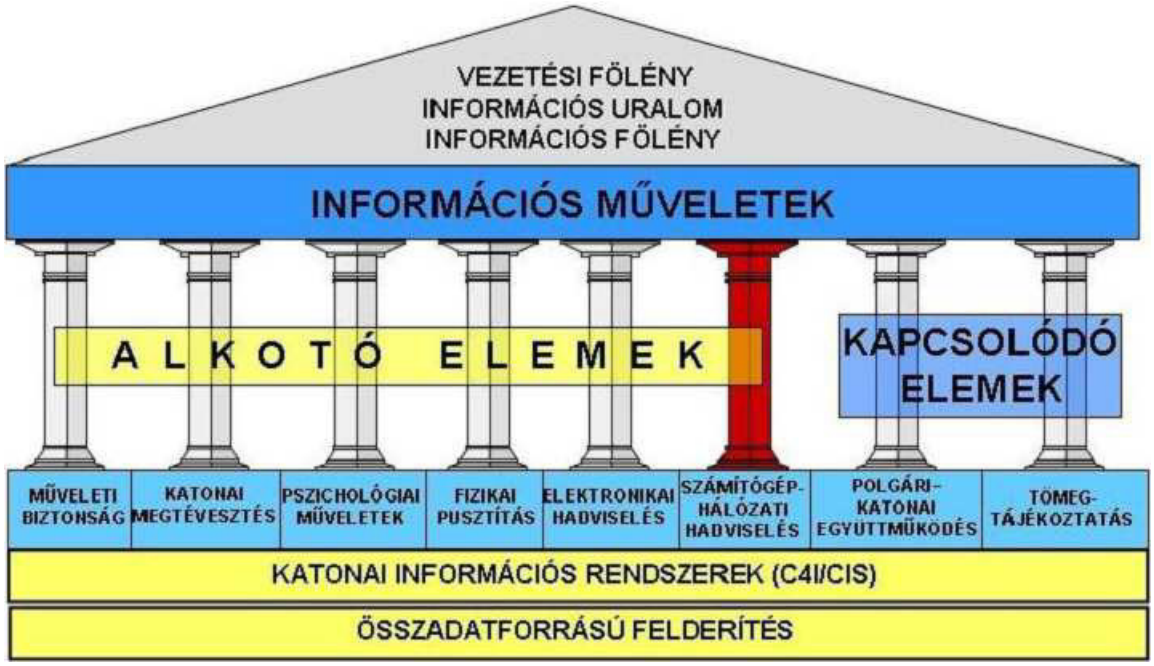
Mivel dolgozatomat a Katonai Műszaki Doktori Iskola keretén belül írom az információtechnológiai környezetben elkövetett támadások és bűncselekmények krimináltechnikai vizsgálatáról, ezért szükséges elemeznem azt, hogy az általam tanulmányozott magatartásformáknak milyen kapcsolatuk van a katonai műveletekkel, ezek milyen kapcsolatban állnak a jogtudománnyal.

[17] Általánosan forenzikus, illetve az angol szakirodalom alapján gyakran „IT forensics” vagy „computer forensics”-ként emlegetett tudomány.

I.1.1 Támadások információtechnológiai környezetben

Az információtechnológiai környezetben végrehajtott támadások jellemzőinek feltárásakor az értekezésemben felhasznált kiindulási alap az információs műveletekkel kapcsolatos kutatások voltak. Információs műveletek alatt *„azon koordinált tevékenységeket értjük, amelyek a szemben álló fél információira, információ alapú folyamataira és infokommunikációs rendszereire gyakorolt hatásokkal képesek támogatni a döntéshozókat, a politikai, gazdasági és katonai célkitűzéseik elérésében úgy, hogy e mellett a saját hasonló folyamatukat és rendszereket hatékonyan kihasználják és megóvják”*. [24 p. 185]

Az információs műveletek összefoglalását az alábbi ábra mutatja be:



1. ábra – Információs műveletek elemei
(forrás: [26])

Az informatikai igazságügyi szakértők számára azonban az információs műveletek értelmezése túlságosan széles, mivel olyan kompetenciaterületeket is lefed, amelyek nem tartoznak az informatika tudományterületéhez. Ehhez legközelebb az információs műveletek elemei/képességei közül a számítógép-hálózati hadviselés áll, ez az a terület, ami az értekezésem szempontjából releváns. A vonatkozó szakirodalom szerint *„Számítógép-hálózati hadviselés egyrészt a szemben álló fél hálózatba kötött informatikai rendszerei működésének befolyásolására, lerontására, lehetetlenné tételére irányul, másrészt viszont*

a saját hasonló rendszerek működésének fenntartására törekszik. […] A ~ magában foglalja:

- *a számítógépes hálózatok struktúrájának feltérképezését;*
- *a forgalmi jellemzőjük alapján a hierarchikus és működési sajátosságok feltárását;*
- *a hálózaton folytatott adatáramlás tartalmának regisztrálását;*
- *a hálózatokban folyó megtévesztő, zavaró tevékenységet;*
- *a célobjektumok program- és adattartalmának megváltoztatását, megsemmisítését valamint*
- *a szemben álló fél hasonló tevékenysége elleni védelem kérdéseit."* [24 p. 228]

A számítógép-hálózati hadviselés tevékenységei életciklusszerűen ~ felderítési ~ támadási és ~ védelmi osztályokba sorolhatók.

„A számítógép-hálózati támadás szoftveres vagy hardveres úton való behatolást jelent a szemben álló fél számítógépes rendszereibe, illetve hálózataiba azzal a céllal, hogy tönkretegyük, módosítsuk, manipuláljuk, vagy hozzáférhetetlenné tegyük az adatbázisban tárolt adatokat, információkat, illetve magát a rendszert vagy hálózatot. A támadás a számítógép hálózati elemekben való fizikai károkozást is jelentheti, amelyet a szoftverek módosításával vagy manipulációjával lehet elérni." [24 pp. 228–229]

A számítógép-hálózati hadviseléssel foglalkozó hazai szakirodalom még nem tárta fel az ezzel kapcsolatos teljes körű támadási taxonómiát. Jelenleg nincs egységes, valamennyi lényeges jellemzőt leíró rendszertan, ezzel a legfrissebb kutatások is elsősorban valamely részterületre koncentrálva foglalkoznak. [25] [26] [27] A hazai szakirodalom továbbá elsősorban a hadtudomány sajátos szempontjait helyezi előtérbe. Ezzel szemben az informatikusok, az üzleti élet szereplői, a köznyelv, de esetenként a hazai hadtudományi szerzők is több olyan magatartást is támadásként értékelnek, amelyeket itt mindenképp figyelembe kell venni. Ide tartoznak a „cybertámadások", amelyeket szándékosan elkövethetnek terroristák[18], államok[19], bizonytalan státuszú szervezetek[20], illetve magánszemélyek[21]. [28] [29] [30] [31] [32] [33]

[18] Az első dokumentált „cyber-terrortámadás": Elalam Tamil Tigrisei. Srí Lanka, 1997.

[19] L. orosz–grúz kiberkonfliktus. 2008.

[20] Az Anonymus külföldön is és hazánkban is több cég vagy hivatal információtechnológiai rendszerének működését befolyásolta vagy módosította, nyilvánosságra hozta az adatait.

[21] Reonel Ramones és Onel de Guzman „ILOVEU" vírus, Fülöp-szigetek, 2000.

A szándékos támadók mellett a mai támadási módszerekben jelentős szerepet kapnak az ún. zombi számítógépek is, amelyek olyan személyek birtokában vannak, akik ugyan fizikailag birtokolnak egy-egy információtechnológiai eszközt, azonban a tényleges logikai kontrollt[22] külső személy vagy szervezet gyakorolja az eszköz felett[23]. [27] [34]

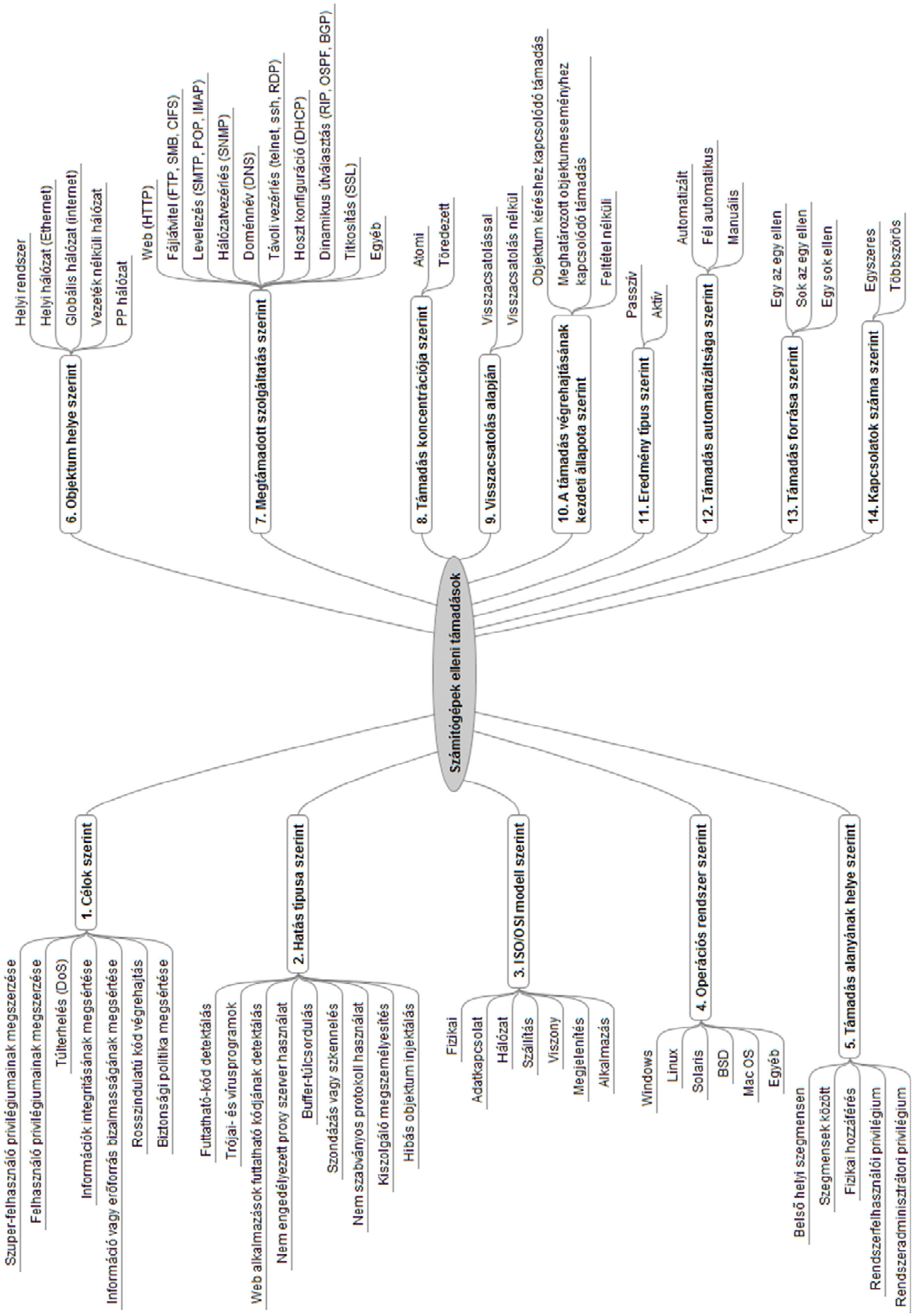
A támadások végrehajtásában – az internet architektúrájának technológiai sajátosságai miatt – részt vesznek továbbá technikai feladatokat ellátó információtechnológiai eszközök[24]. Ezek nincsenek sem a támadó, sem pedig a megtámadott uralma alatt, hanem valamilyen harmadik fél, általánosságban az internetszolgáltatók üzemeltetésében és felügyelete alatt működnek. Ezeket az eszközöket rendszerint professzionális, az információbiztonság terén megfelelő ismeretekkel rendelkező rendszergazdák konfigurálják és üzemeltetik, emellett jellemzően naplózzák is a működésüket. Ezek a naplók egy támadást követően felhasználhatók a támadás körülményeinek kivizsgálására.

A külföldi szakirodalomban több olyan rendszertan is megtalálható, amely a számítógépek elleni támadások osztályozását tűzte ki célul. Ezek közül számomra a legadekvátabb a Paulauskas és Garsva által kidolgozott modell, tekintettel arra, hogy a támadások valamennyi lényeges jellemzőjét azonosítja (célok, típusok stb. szerint). [35] A modell véleményem szerint jó kiindulási alap nemcsak hagyományos számítógépek, hanem az általános információtechnológiai eszközök elleni támadások technikai vizsgálatának rendszerezéséhez. A modell összefoglalását a 2. ábra mutatja be.

[22] Rendszerint adminisztrátori privilégiumokkal.

[23] A zombi gép tulajdonosa/üzemeltetője szempontjából a támadás nem szándékos, inkább gondatlan magatartás következménye.

[24] Főleg a számítógép hálózati forgalmának vezérlését, kontrollját ellátó eszközök: útválasztók, hálózati kapcsolók, tűzfalak stb.



2. ábra – Számítógépek elleni támadások osztályozása ([35] alapján szerk.: Illési Zsolt)

A fentiek alapján megállapítottam, hogy a számítógép-hálózati hadviselés „támadás" fogalma értekezésem szempontjából mindenképp megszorító. Nem foglalkozik a békeidőben, esetleg nem katonai egységek által végrehajtott műveletekkel, illetve nem tartalmazzák a támadásokban aktívan, de a támadásban nem szándékosan résztvevő szereplőket. A katonai műszaki gyakorlatban a számítógép-hálózati hadviselésben alkalmazott módszertanok, technikák és eszközök alapvetően nem térnek el a terroristák, a bűnözők vagy politikai célból létrejött szervezetek által használtaktól. A különbség főleg a motivációban[25], a célpontok kiválasztásában[26], az elkövetőben[27], illetve a végrehajtás módjában[28] van. [36]

Az értekezésemben ezért tágabban értelmezem az információtechnológiai környezetben elkövetett támadásokat. Mivel a támadó célpontja egy információtechnológiai rendszer, annak komponense vagy annak adatai és támadásai végeredményképpen az

- információszerzési,
- információ felhasználási,
- információ előállítási,
- információtovábbítási,
- információtárolási,
- információfeldolgozási

tevékenységeket sérti vagy veszélyezteti. Éppen ezért **a továbbiakban az „információtechnológiai környezetben elkövetett támadás" megnevezést használom,** és a támadás kontextusába beleértem a támadót, a célpontot, a támadási közegként vagy eszközként felhasznált információtechnológiai rendszert, azok elemeit és technológiai sajátosságait. [37] Mivel értekezésem az informatikai igazságügyi szakértők szempontjából, az ehhez tartozó kompetenciák alapján vizsgálja a témát, ezért a továbbiakban csak az információtechnikai, technológiai elemekkel foglalkozom.

[25] Elsődleges motivációs tényezők: pénzügyi, politikai.

[26] Állami, kormányzati, katonai, vagy bármilyen egyéb célpont.

[27] Az elkövető lehet nemzeti vagy nemzetközi szervezet, egyén.

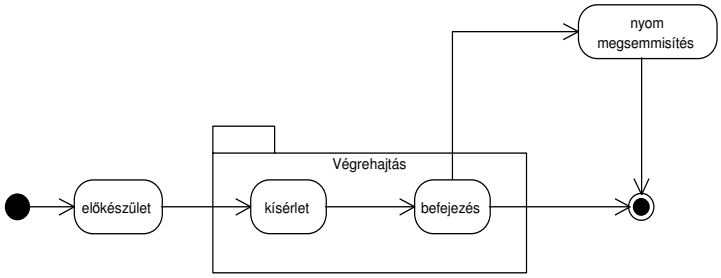
[28] Erőszakmentes, az erőszaknak, mint az elkövetést megkönnyítő eszköznek az alkalmazása, a félelem mint szimbólum alkalmazása.

I.1.2 Bűncselekmények információtechnológiai környezetben

Jelenleg az információtechnológiai környezetben elkövetett támadások és bűncselekmények osztályozásával és rendszerezésével a jogi szakirodalom – elsősorban a bűncselekmények konkrét megjelenési formái, valamint a veszélyeztetett értékek és jogtárgyak sokszínűsége miatt – adós maradt. Nincs általánosan elfogadott fogalma sem az információtechnológiai rendszerek támadásának, sem az ebben a környezetben elkövetett bűncselekményeknek. [38]

Az információtechnológiai rendszerek komplexitása miatt nem csak az elkövetők (a továbbiakban: elkövető vagy terhelt) kerülhetnek a nyomozóhatóság látókörébe, hanem ártatlan, egy információtechnológiai rendszer informatikához, információbiztonsághoz hozzá nem értő tulajdonosai, üzemeltetői is. Ugyanis az elkövetés valamelyik tárgya, vagy az információtechnológiai környezetben elkövetett bűncselekmény (virtuális) helyszínének elemei lehetnek olyan számítógépek, amelyeket a bűnelkövetők „hekkeltek" meg, használták fel. [27] [34] Az információtechnológiai környezetben elkövetett támadásoknál leírtakkal analóg módon tehát megállapítható, hogy a bűncselekmények virtuális helyszíne magába foglalja az elkövetői, a sértetti, a támadási közegként vagy eszközként felhasznált információtechnológiai rendszereket, azok elemeit és technológiai sajátosságait.

A bűncselekményeknek megvan a sajátos életciklusa: az elkövető megtervezi és előkészíti, majd végrehajtja azt, később ha lehetősége (és intelligenciája) engedi, akkor a keletkezett nyomokat megsemmisítve próbálja meg ellehetetleníteni a sikeres büntetőeljárást. Ezt az életciklust mutatja be a 3. ábra.



3. ábra – A bűncselekmények állapotdiagramja (szerk.: Illési Zsolt)

Információtechnológiai környezetben elkövetett bűncselekmények sajátossága a(z)

- **gyorsaság** – vagyis az eredmények rövid idő alatt, nagy távolságban, jelentős kárt okozva jelennek meg, bár egy-egy bűncselekmény előkészületére az elkövető jelentős időt használ(hat) fel,
- **magas látencia** – vagyis az információtechnológiai környezetben elkövetett bűncselekmények sértettjei nem minden esetben érzékelik közvetlenül az okozott károkat, nem, vagy csak részben fedezik fel az ellenük elkövetett támadást vagy bűncselekményt, illetve azokat nem jelentik a hatóságoknak,
- **nemzetköziség** – vagyis az információtechnológiai környezetben elkövetett támadások gyakran átnyúlnak a természetes országhatárokon, így az elkövető, a sértett és az esetleg felhasznált eszközök más-más állam joghatósága alá tartoznak,
- **intellektuális jelleg** – vagyis az elkövetők általában jól képzett, intelligens személyek, akik tisztában vannak cselekményük következményeivel, a felderítés elleni védelem szükségességével és annak módszereivel. [39] [4]

Kriminológiai szempontból egy információtechnológiai rendszer, annak hardver, szoftver komponense[29], számítógép-hálózata vagy annak szegmense[30] lehet:

- **célpont** – ha az elkövető célja a hardver vagy szoftver jogellenes módosítása, eltulajdonítása, tönkretétele;
- **megvalósítási/elkövetési tárgy/környezet**, ha az elkövető a jogellenes cselekményt egy információtechnológiai rendszeren belül, annak felhasználásával követi el;
- **elkövetést/megvalósítást megkönnyítő eszköz**, ha az elkövető a jogellenes cselekményének kitervelésére, nyomainak eltüntetésére használja fel a rendszert, vagy annak komponenseit;
- **elkövetés szimbóluma**, ha az elkövető jogellenes cselekményének nem közvetlen tárgya egy információtechnológiai rendszer vagy eszköz, de a bűncselekmény során a

[29] Szoftverkomponens alatt olyan önálló szoftver összetevőt értek, amely jól elhatárolható a környezetétől (a rendszerben telepített egyéb szoftver összetevőktől), rendszerint függetlenül telepíthető, vagy függetlenül futtatható, zárt funkcionalitással rendelkezik. Az értekezésemben használt definíció szerint azonban a komponens nem elemi szoftverösszetevő, hanem lehet komplex rendszer (pl. operációs rendszer, ERP rendszer) is. Ebben az esetben ennek a komplex szoftverkomponensnek az alrendszerei is szoftver komponensként értelmezhetők (pl. operációsrendszer esetén a segédprogramjai, ERP rendszer esetén az üzleti logikát tartalmazó egyes modulok, továbbá a rendszert támogató adatbázis).

[30] Ethernet hálózat esetén szegmens a hálózat ütközési tartománya; általánosságban a szegmens a számítógép-hálózat azon része, amelyben minden eszköz ugyanazt a fizikai réteget használva kommunikál egymással.

terhelt valamilyen hardver, szoftver eszközre vagy számítógép-hálózatra hivatkozva vezeti félre a sértettet[31].

[39] [40]

Saját szakmai tapasztalataim alapján javaslom kiegészíteni ezt a felsorolást egy további elemmel, amikor az információtechnológiai rendszer, annak hardver, szoftver komponense, számítógép hálózata vagy annak szegmense lehet az

- **elkövetés tanúja**, ha a bűncselekménnyel összefüggésben lévő bizonyítékként felhasználható releváns adatot rögzít egy információtechnológiai eszköz. Függetlenül attól, hogy a tettes célja egy információtechnológiai rendszer valamely komponense volt-e vagy sem, használt-e információtechnológiai eszközt az elkövetéshez vagy sem[32]. [40]

Mivel egy információtechnológiai rendszer komplex módon kapcsolódhat a bűncselekményekhez, ezért – egyéb jogi specifikáció hiányában – a továbbiakban azokkal az esetekkel foglalkozom, amelyeknél fenti felsorolás szerinti öt sajátosság közül legalább egy megtalálható. Azaz: az információtechnológiai rendszer vagy komponense aktív, passzív módon részt vett egy bűncselekményben, vagy rögzítette a bűncselekmény valamely releváns attribútumát.

Ezen a bűncselekmények azonosítására – az információtechnológiai környezetben elkövetett támadásoknál leírtakkal analóg értelmezés alapján – a továbbiakban az „információtechnológiai környezetben elkövetett bűncselekmény” megnevezést használom, és csak az információtechnikai, technológiai elemekkel foglalkozom. Információtechnológiai környezetben elkövetett bűncselekménynek minősülnek tehát azok az előző alfejezetben ismertetett támadások, amelyre a törvény büntetés kiszabását rendeli. Nem tartoznak viszont ide azok az információtechnológiai környezetben elkövetett támadások, amelyeket a fegyveres összetűzések joga alapján jogszerűen vívnak meg a felek. [7]

---

[31] Erre példa az 1978. évi IV. törvény a Büntető Törvénykönyvről – a továbbiakban Btk. – 318. §-nak megfelelően csalásnak minősülő eset, ahol az elkövető nem létező számítógépeket ad el a sértettnek.

[32] Ha az internetszolgáltató hálózati eszközei naplózzák egy, a Btk. 261. §-a alapján terrorcselekmény valamely lényeges körülményét, vagy elektronikus hang és/vagy képfelvétel készül egy, a Btk. 197. §-a szerinti erőszakos közösülésről, vagy az elkövetők elektronikus levelezés során terveznek meg egy, a Btk. 166. §-a szerinti emberölést – és a postaláda megőrzi a levélváltást.

I.2 Bizonyítás és bizonyíték

A polgári és büntető ügyekben az eljárás résztvevőinek[33] célja, hogy a per tárgyává tett polgári jogi vagy büntetőjogi tényállás igaz vagy hamis voltát igazolandó adatokat, bizonyítékokat felkutassák, összegyűjtsék, és a bíróság rendelkezésére bocsássák[34].

A bíróságnak az elé tárt bizonyítékok alapján kell kialakítania a véleményét, meghoznia a döntését. Ezért aki a polgári jog vagy a büntetőjog megsértőivel szemben fel akar lépni, annak nem elegendő az, hogy „igaza van", hanem elegendő mennyiségű és minőségű bizonyítékot is kell szolgáltatnia az érvelésének alátámasztására.

A rendőrség, ügyészség vagy egyéb nyomozásra feljogosított szerv a vizsgálatai során nyomozhat mind bűnös, mind bűntelen gyanúsítottak után, ezért lényeges kérdés, hogy az üggyel kapcsolatos valamennyi releváns tényt, adatot összegyűjtsön. A nyomozást végzők feladata nem kizárólag a koncepcióikat alátámasztó, csupán a vádhatóság igényeit kiszolgáló terhelő bizonyítékok, hanem a terheltet mentő bizonyítékok feltárása is. Nevezetesen, hogy lehetőleg ártatlan emberek ellen ne induljon büntetőeljárás, vagy ha jogosan indult, akkor a büntetések legyenek arányosak az elkövetett bűncselekmények társadalomra veszélyességével és tárgyi súlyával. [21]

A bizonyítás módja, a felhasználható eszközök részben eltérnek az egyes jogágakban, ezért az alábbiakban összefoglalom a polgári jogi és a büntetőjogi bizonyítékszerzés, bizonyítás sajátosságait, összehasonlítom a polgári jog és a büntetőjog bizonyítás szempontjából legfontosabb alapfogalmait:

- bizonyítás, bizonyítási eljárás,
- bizonyítási eszköz és bizonyíték,
- bizonyítási teher,
- bizonyítási tilalmak.

I.2.1 Bizonyítás, bizonyítási eljárás

A bizonyítás egy sajátos megismerési folyamat, ami főleg – az egyedi ügyek tényállásával kapcsolatos – múltbeli eseményeknek a valóságnak megfelelő megállapítására, utóla-

[33] A felek, hatóságok, vagy esetenként a per egyéb résztvevői.

[34] A büntetőeljárás és bizonyítás szabályait az 1998. évi XIX. törvény a továbbiakban „Be", a Polgári perrendtartás és bizonyítás szabályait a 1952. évi III. törvény, a továbbiakban „Pp" tartalmazza.

gos rekonstrukciójára irányul, és bizonyítékok összegyűjtésével, vizsgálatával és azok mérlegelésével kapcsolatos tevékenységekből áll.

A bizonyítási eljárást büntetőügyben az eljáró hatóság, esetenként a (pót)magánvádló folytat, amíg polgári ügyben a keresetet benyújtó fél, azaz a felperes, vagy a viszontkeresetet benyújtó fél.

Büntető ügyekben a hatósági szerepkörrel nem rendelkező félnek (a sértettnek) korlátozottak a lehetőségei a törvényes bizonyítékgyűjtésre, azaz információtechnológiai rendszerekben folyó tevékenységet naplózhat ugyan, de nincs lehetősége például az adatforgalom lehallgatására, mert az jogszerűtlen bizonyítékként kizáródhat a tárgyalásból. Büntető ügyben tehát célszerű a gyanú megfogalmazódását követően konzerválni, rögzíteni az információtechnológiai rendszer adatait[35], és ezt követően feljelentést tenni, illetve további eljárási cselekményt lefolytatni. Amennyiben a gyanúokot a feljelentésben megfelelően támasztja alá a sértett, és biztosítja a saját birtokában lévő rendszerek szakszerűen lementett adatait, a hatóság a többlet (nyomozati) jogosultságait felhasználva eredményesen derítheti fel a bűncselekményt és vonhatja felelősségre az elkövetőt. Amennyiben törvénytelen bizonyítékszerzés vagy szakszerűtlen beavatkozások miatt nem lehet felhasználni az információtechnológiai rendszerben megtalálható információkat, úgy a büntetőeljárásokra oly jellemző „bizonyítékínség" miatt lehet, hogy sikertelen lesz a vádemelés és a felelősségre vonás.

Polgári perekben hasonlóan kell eljárni, hiszen ilyenkor is megfelelő hitelességű, minőségű és mennyiségű adatot kell a bíróság elé tárni, hogy egyértelműen meggyőzzük az igazunkról.

Bár elvileg mind a polgári, mind a büntető bíróságok szabadon mérlegelhetik az egyes bizonyítási eszközöket, vannak preferált eszközök. Emiatt a technikai jellegű területeken kirendelt igazságügyi szakértőket rendszerint magasabbra értékelik a bíróságok a valamely fél által megbízott igazságügyi szakértőknél, és még magasabbra, mint az eseti szakértők szakvéleményeit. Érdemes tehát megfontolni, hogy milyen bizonyítási eszközöket és milyen módon kíván valaki felhasználni, mielőtt egy polgári vagy büntetőügybe belefogna. [41] [42]

[35] A későbbiekben leírt eszközökkel, módszerekkel.

I.2.2 Bizonyítási eszköz és bizonyíték

A polgári eljárásban a bizonyítás tárgya elsősorban valamelyik fél keresetét, illetve a felperes vagy az alperes viszontkeresetét megalapozó, vagy a keresettel (viszontkeresettel) szembeni védekezést megalapozó tények. [42 p. 29]

Polgári perekben a bizonyítandó tények lehetnek eljárásjogi tények[36], a keresettel kapcsolatos történésekkel, tárgyi jelenségekkel kapcsolatos, illetve szubjektív mozzanatok.

A büntetőeljárásban a bizonyítékok *„olyan adatok,*

a) amelyek büntetőjogilag releváns tényekre vonatkoznak,

b) amelyeket a törvény által megengedett forrásokból szereznek be,

s éppen ezért összességükben és összefüggésükben felhasználhatók (alkalmasak) a büntetőjogilag releváns tényállásnak az ügydöntő hatóság általi megállapítására, utólagos rekonstrukciójára (eljárásjogi bizonyíték)”. [41 p. 79]

A bizonyítás során mind a polgári, mind a büntető bizonyítás során az objektív elemek mellett jelentős szerepet játszanak a szubjektív, az emberi lelkivilággal kapcsolatos tények is, mivel ezeknek jelentős szerepük van a tényállás bírói megítélésében.

Szubjektív tényállási elem mind polgári, mind büntető jogban az akarat, a szándék, a beszámíthatóság, a tudatosság. Polgári ügyekben jelentős szerep jut a jóhiszeműségnek, rosszhiszeműségnek, az egyetértés meglétének vagy hiányának, az elvárhatóságnak, vagy az el nem várhatóságnak. Büntető ügyekben továbbá jelentős szubjektív tényállási elem a motívum[37].

Általában nem kell bizonyítani a köztudomású tényeket, illetve azokat a tényeket, amelyről az eljáró hatóságnak tudomása van, továbbá nem kell bizonyítani a jogszabályokat sem.

A polgári és a büntető joggyakorlatban az alapvető különbség az, hogy amíg a polgári perben a bíróság megelégedhet a valószínűség magasabb fokával, addig a büntetőbíráknak az ítélet meghozatalakor kétséget kizáróan kell meggyőződnie a bűnösségről a tény-

[36] Például a bíróság hatás- és illetékességi körére vonatkozók, a felek jogképességére, cselekvőképességére vonatkozók.

[37] Aljas indok, bosszú, rasszizmus, féltékenység, szexuális indíték stb.

állás alapos, hiánytalan és a valóságnak megfelelő tisztázásával, és ha nem látja bizonyítottnak a tényállási elemet, akkor azt a terhelt javára kell értékelnie (in dubio pro reo).[38]

A bizonyítási eszközök azok a polgári vagy büntetőeljárási cselekmények vagy dolgok, amelyekből a hatóság, bíróság illetve az eljárás résztvevői a keresetre, (illetve a viszontkeresetre) vagy bűncselekményre, a felekre vagy az elkövetőre vonatkozó ismereteket szereznek. A jogi szakirodalomban a bizonyítási eszköz kifejezés szinonimájaként a bizonyítékforrást is használják, azaz, mint olyan eszközre történő utalást, amelyből a bizonyíték ered.

Mind a büntetőeljárási jog, mind a polgári perrendtartás meghatározza a felhasználható bizonyítási eszközök körét, az alábbiak szerint:

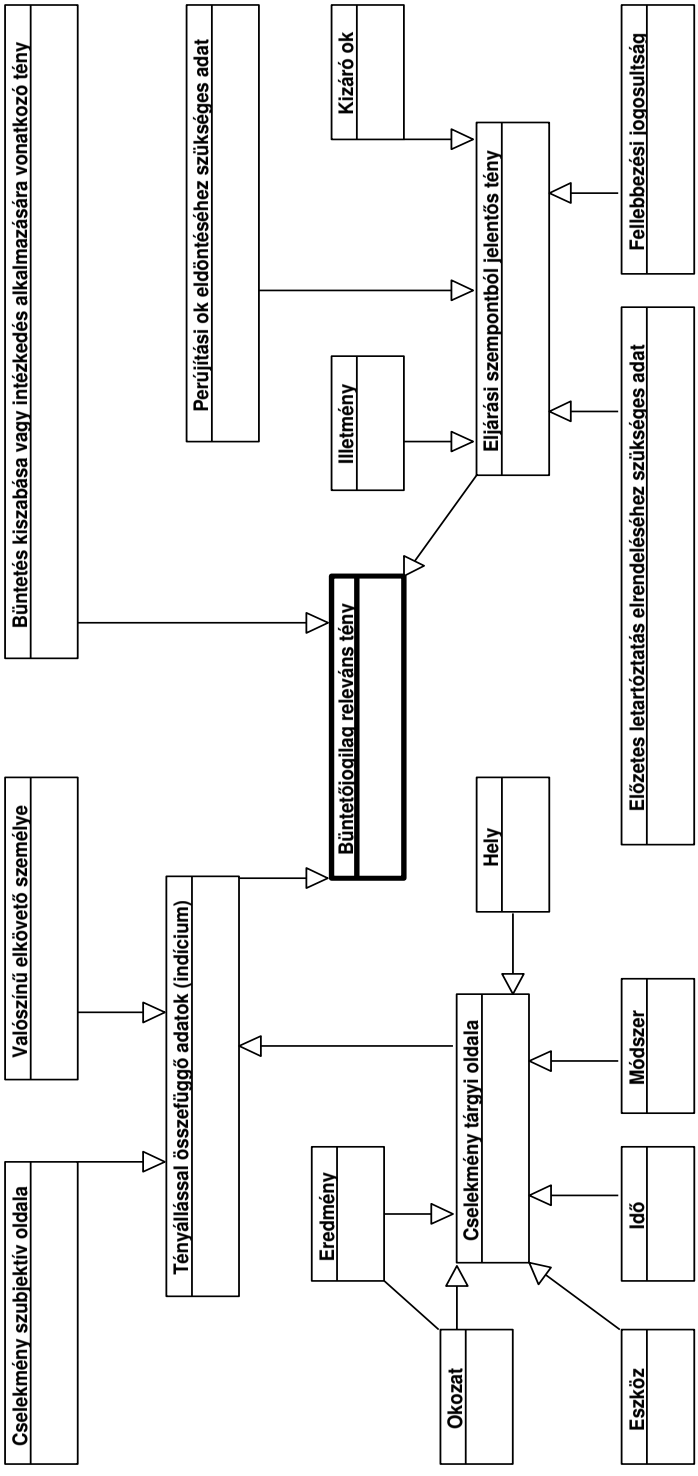
Pp 166. § (1)	*Be. 76. § (1)*
Bizonyítási eszközök különösen	*A bizonyítás eszközei*
a tanúvallomások	*a tanúvallomás*
a szakértői vélemények	*a szakvélemény*
a szemlék	
az okiratok	*az okirat*
tárgyi bizonyítékok	*a tárgyi bizonyítási eszköz*
	terhelt vallomása

A Pp. 3. § (5) további bizonyítási eszközt is meghatároz, azaz: *„Ha törvény másként nem rendelkezik, a bíróság a polgári perben alakszerű bizonyítási szabályokhoz, a bizonyítás meghatározott módjához vagy meghatározott bizonyítási eszközök alkalmazásához nincs kötve, szabadon felhasználhatja a felek előadásait, valamint felhasználhat minden egyéb bizonyítékot, amely a tényállás felderítésére alkalmas."* [43]

A Be. 78. § (1) ezzel szemben nem ilyen megengedő: *„A büntetőeljárásban szabadon felhasználható a törvényben meghatározott minden bizonyítási eszköz, és szabadon alkalmazható minden bizonyítási eljárás"*, tehát a büntetőeljárásban felhasználható bizonyítékforrások köre zárt. [44] [41] [42]

[38] A nemzetközi jogi irodalom egyik legjelentősebb ítélete a fenti kettősséggel kapcsolatban O. J. Simpson ügyében született, akit a felesége és annak barátja ellen elkövetett emberölés miatt indított büntetőügyben felmentettek, de ugyanebben a tárgyban a feleség családja által indított kártérítési (polgári) perben több tízmillió dollár kártérítés megfizetésére kötelezett a bíróság.

A támadásokkal és bűncselekményekkel kapcsolatban a bizonyíték tehát büntetőjogilag releváns tény, amelynek elkészítettem a következő ábrán látható „csontváz” osztálydiagramját:



4. ábra – Büntetőjogilag releváns tények osztálydiagramja ([45] alapján szerk.: Illési Zsolt)

I.2.3 Bizonyítási teher

Az eljáró bíróság sem a polgári, sem a büntető eljárás során nem köteles vádat vagy keresetet alátámasztó bizonyítékot szolgáltatni. Polgári perben a bizonyítással együtt járó feladatok teljesítése (a bizonyítási teher) a keresetet vagy viszontkeresetet benyújtó felet terheli. A bizonyításnak a polgári perrendtartás alapján, mint azt már korábban is említettem, nem kell minden kétséget kizárónak lennie, gyakran elegendő valamely tény valószínűségének az igazolása. A büntetőeljárás során a bizonyítási teher a vádlót vagy a vádhatóságot terheli, a bizonyítás egyik fő pillére az ártatlanság vélelme, amely alapján a vádlott javára kell értékelni minden nem bizonyított tényt.

Elvileg tehát a „per ura" minden esetben az, aki valamilyen tényt állít, és a Pp. vagy a Be. az ő feladatává teszi a bizonyítást. Polgári perben azonban gyakran sérül ez az elv, és a bíróság megkülönböztetett szerepet játszik a bizonyításban (például a kirendelt szakértők kontra a megbízó szakértője által beadott szakvéleményének elbírálása során). [46]

I.2.4 Bizonyítási tilalmak

A polgári perben a bíróságot egyetlen a jogszabályban is nevesített tilalom köti, a Pp. 166. § (2), amely szerint *„Eskünek a perben helye nincs"*. Ez a tilalom törvényi szinten csakis azért indokolt, mert a szakrális eskü és az ehhez kapcsolódó következmények közel ezer évig rányomták bélyegüket a büntető és polgári eljárásra egyaránt. [43] [46]

A büntető eljárás a polgári perrendtartással szemben nem egy, hanem több olyan pontot tartalmaz, amelyek közvetlenül vagy közvetve bizonyítási tilalmakat határoznak meg. Ezek között vannak „íratlan" tilalmak, azaz: nem lehet bizonyítani azokat a tényeket, állításokat, amelyek ellentétesek valamely megdönthetetlen törvényi vélelemmel, vagy ellentétesek igazolt egzakt tudományos tételekkel vagy elismert emberi tapasztalatokkal.

Vannak burkolt, más jogszabályokkal együttesen megjelenő tilalmak. Például nem hallgatható ki a védő arról, amit vele a védence közölt, illetve nem hallgatható ki az állami, szolgálati titok tudója olyan titkokkal kapcsolatban, amelyek elmondása alól nem mentesítette a titokgazda.

A Be. meghatároz továbbá olyan tilalmakat is, amelyek a bizonyítási eszközökkel kapcsolatosak. Ezek között vannak abszolút tilalmak, mint a védő kihallgatásának tilalma és a védői iratok lefoglalásának tilalma. Vannak relatív tilalmak is, amelyek feloldhatók, például a vallomás megtagadására jogosult tanú kihallgatható, ha a kihallgatásba bele-

egyezik. A bizonyítási eszközökkel kapcsolatos speciális tilalom továbbá, hogy a gyanúsítottnak nem lehet jogszerűtlen ígéretet tenni a kihallgatás során a vallomásért cserébe, illetve nem lehet olyan kérdést feltenni, amely nem bizonyított tényállási elemeket is tartalmaz (sugalmazva a vallomástételt) (Be. 180.§ (1) bekezdés).

Sajátos büntetőeljárási szabály vonatkozik a poligráf alkalmazására. A (Be. 180.§ (2) bekezdés és a 182.§ (2) bekezdés alapján hazugságvizsgáló csak a terhelt beleegyezése mellett, szaktanácsadó igénybevételével használható. A többi alkalmazás ezek alapján nem megengedett, sőt amennyiben fiatalkorúak érintettek, úgy a törvény kifejezetten meg is tiltja a poligráf alkalmazását (453.§ (3) bekezdés).

A büntetőeljárás során alkalmazandó a „mérgezett fa gyümölcse" elv, azaz, a bizonyíték megszerzésével és értékelésével kapcsolatos tilalom, amely alapján kizárandók egyes jogellenesen szerzett bizonyítási eljárási eszközök. *„Nem értékelhető bizonyítékként az olyan bizonyítási eszközből származó tény, amelyet a bíróság, az ügyész vagy a nyomozó hatóság bűncselekmény útján, más tiltott módon vagy a résztvevők eljárási jogainak lényeges korlátozásával szerzett meg."* (Be. 78.§ (4) bekezdés). A mérgezett fa gyümölcse elvének értékelésekor a jogalkalmazás során érdemben mérlegelni kell azt is, hogy a jog szabályainak megszegése mennyiben volt befolyással a bizonyításra. Ha a jogsértés csak „technikai jellegű", és nem érinti a bizonyítás vagy az eljárás érdemi részét, akkor az nem indokolja egyértelműen az így szerzett bizonyíték kizárását.

A titkos adatszerzéssel (például lehallgatással) szerzett bizonyíték – ha az adatgyűjtés nem a jogszabályok által meghatározott módon és feltételek betartása mellett történt – a fenti joghelyre való tekintettel szintén nem használható fel bizonyítékként. [44] [45]

I.3 Nyomok

A bizonyítékkal és a bizonyítással kapcsolatban leírtakból látható, hogy az eredményes és hatékony jogi eljárásban szükséges, hogy a megfelelő mennyiségű és minőségű bizonyítékok rendelkezésre álljanak. Az információtechnológiai eszközökkel és rendszerekkel kapcsolatban a bizonyíték az azokban tárolt, feldolgozott vagy az azokon keresztül továbbított adatokból nyerhető, ezért fontos megismerni a bizonyítékok megszerzésének módszertani hátterét.

A büntetőeljárás során szerzett bizonyítékokkal szemben támasztott szigorúbb körülmények miatt mindenhol az igazságügyi szakértői, bűnügyi technikai vizsgálatok hatá-

rozzák meg azt, hogy a tudomány és a technika aktuális állása mellett hogyan lehet bizonyítékot szerezni információtechnológiai, illetve kommunikációs rendszerekből. Ezért a dokumentum további részében a vizsgálatok kereteit a bűnügyi nyomozástan, a kriminalisztika szemszögéből tanulmányozom, és az informatikai igazságügyi szakértő feladatain keresztül mutatom be.

A kriminalisztika a *„bűnügyi nyomozástan, azaz a bűnügyi tudományoknak az az ága, amely a bűncselekmények felderítésének és bizonyításának eszközeit és módszereit tárja fel és rendezi elvi és gyakorlati szempontból egyaránt”*. [47 p. 19]

A kriminalisztikát két fő részre, általános és különös részre osztva tárgyalják. Az **általános rész** öt területre tagolható:

1) ***Kriminalisztika történet*** – amely azzal foglalkozik, hogy történelmileg hogyan alakult ki és fejlődött:
   - a bűnüldözés szervezeti rendszere,
   - a kriminalisztika módszerei,
   - a természettudomány, a műszaki-technikai tudományok és a bűnfelderítés kapcsolata.
2) ***Kriminalisztikai elmélet*** – ide tartozik a kriminalisztika egészére érvényes, általános érvényű tételek kidolgozása, amelyek alapvetően befolyásolják e tudományterület valamennyi eredményét.
3) ***Krimináltechnika*** – amelynek célja a bűncselekmények megelőzése, felderítése és bizonyítása érdekében a bizonyítási eszközök felkutatása, rögzítése és vizsgálata a technika módszereivel és eszközeivel. A krimináltechnika foglalkozik továbbá a tárgyi bizonyítási eszközök létrejöttének törvényszerűségeivel is. [48 p. 63] Az igazságügyi szakértők, így az informatikai igazságügyi szakértők is ezen a területen végzik a forenzikus tevékenységeiket.

   A krimináltechnikai tevékenységnek három fő iránya van:
   - büntető eljárások során a bizonyítékok felkutatása, rögzítése és szakértői vizsgálata,
   - a bűncselekmények megelőzésének előmozdítására technikai eszközök kifejlesztése, azok működésének ellenőrzése és gyakorlati alkalmazása,
   - tudományos kutató-, fejlesztő munka végzése.
4) ***Krimináltaktika***, a személyi jellegű bizonyítékszerzéssel, annak főbb sajátosságaival és összefüggéseivel foglalkozik.

5) ***Kriminálstratégia***, a politika és a jog által meghatározott, a bűnelkövetést megelőző és korlátozó feladatokat (a kriminálpolitikai elveket) közvetíti az igazságszolgáltatáshoz és az államigazgatási szervezetekhez, valamint előírja a megvalósítás átfogó, tervszerű, koordinált közép- és hosszú távú intézkedéseit.

A **különös rész** az egyes bűncselekmény kategóriák felderítésére és bizonyítására alkalmazható szakkriminalisztikákkal foglalkozik, felhasználva a krimináltechnika és a krimináltaktika általános eredményeit[39]. [48 pp. 58–68] [4]

A kriminalisztikai vizsgálatoknak, ezen belül a krimináltechnikai vizsgálatoknak a célja a törvényes forrásból származó, büntetőjogilag releváns tények szolgáltatása, amelyek összességükben alkalmasak büntetőjogilag releváns tényállás megállapítására. [41 p. 79] Ez a hétköznapi nyelvre lefordítva olyan folyamatot jelent, amely információt nyújt a(z)

- elkövető(k)ről (Ki?)
- események valós természetével kapcsolatban (Mit?)
- események helyszínével kapcsolatban (Hol?)
- események sorrendjével kapcsolatban (Mikor?)
- motivációs tényezőkkel kapcsolatban (Miért?)
- elkövetés módjáról és a felhasznált eszközökről (Hogyan?)

[49 pp. 58–59]

A vizsgálatokat a fenti kérdésekre figyelemmel kell előkészíteni, hogy azok adekvát válaszokat adjanak, és közvetett vagy közvetlen bizonyítékot szolgáltassanak. [48] [41]

A kriminalisztikáról leírtak alapján megállapítottam, hogy az információtechnológiai környezetben elkövetett támadások közül a krimináltechnika csak azokkal foglalkozik, amelyeknek közvetlen büntetőjogi relevanciája van. Értekezésem ezért a továbbiakban az információtechnológiai környezetben elkövetett támadások közül csak a bűncselekményi minősítésű esetekkel foglalkozik[40].

---

[39] Ezáltal a büntetőjog szerkezetével megegyező struktúrában az egyes bűncselekményfajtáknak megfelelő kriminálmetodikai szabályokat és kriminálmetodikai ajánlásokat tartalmaz.

[40] Ez nem jelenti azt, hogy az értekezésemben leírtak nem alkalmazhatók egyéb támadások elemzésére. Épp ellenkezőleg. Mivel a számítógép-hálózati hadviselés és az információtechnológiai környezetben elkövetett (általános) támadások azonos módszereket, technikákat és eszközöket alkalmaznak, a fenti szűkítő értelmezés elsősorban fogalmi egyszerűsítést jelent az értekezésem szempontjából.

I.3.1 Bizonyítékokkal kapcsolatos alapelvek

I.3.1.1 Locard anyagcsere és kölcsönös nyomhagyási szabálya

Edmond Locard az 1920-as évek kiemelkedő kriminalisztikai szakértője szerint bárki, vagy bármi kerül kapcsolatba egy bűncselekmény helyszínével, valamilyen nyomot hagy, és valamilyen nyomot tovább visz magával, amikor elhagyja azt.

Ennek az elvnek (Locard Exchange Principle) a következetes vizsgálata vezetett a traszológia (nyomtan) kifejlődéséhez. A traszológia a krimináltechnikának az az ága, amely a nyomokkal, azok keletkezésének körülményeivel, a nyomképződés folyamatának elemzésével és a nyomképző objektum (tárgy, testrész) azonosításával foglalkozik. A bűncselekmények felderítése, bizonyítása, megelőzése érdekében a nyomok felkutatásának, biztosításának, rögzítésének, vizsgálatának és értékelésének módszereit dolgozza ki.

A nyomtan eredményei az anyagi világban megteremtik az áldozat, terhelt (elkövető) és a helyszín közötti kapcsolatot. [50] [47] A „virtuális" világban is léteznek ilyen nyomok, amelyek hasonló kapcsolatot teremtenek az elkövető, az elkövetésben felhasznált számítógépek és a célpont – a sértett számítógépe – között.

A klasszikus krimináltechnika alapelve az, hogy a nyom keletkezésében három tényező együttesen vesz részt:

- a **nyomképző**, vagyis az a dolog (tárgy vagy testrész), amely a nyomképződési folyamat során a nyomhordozón nyomot hagy,
- a **nyomhordozó**, vagyis az a dolog (tárgy, testrész, talajrész), amelyen a nyomképző a nyomképződési folyamat során nyomot hagy
- a **nyomképződési folyamat**, vagyis a kölcsönhatás módját meghatározó folyamat, amely meghatározza a nyom egyedi jellemzőit, fajtáját.

A krimináltechnikában a nyom és az anyagmaradvány szorosan összefüggő fogalmak, és sok esetben csak a módszer alapján lehet eldönteni, hogy nyom vagy anyagmaradvány vizsgálata történt-e meg, azonban a két fogalom mégsem azonos. Az alábbiak szerint különülnek el:

- **nyom** – a nyomhordozón a nyomképző érintkező felületének formája (alakbeli sajátosság) a vizsgálat tárgya (például harapás)
- **anyagmaradvány** – a nyomhordozón a nyomképző anyaga rakódik le, és ennek elemzése a vizsgálat tárgya (például nyál)

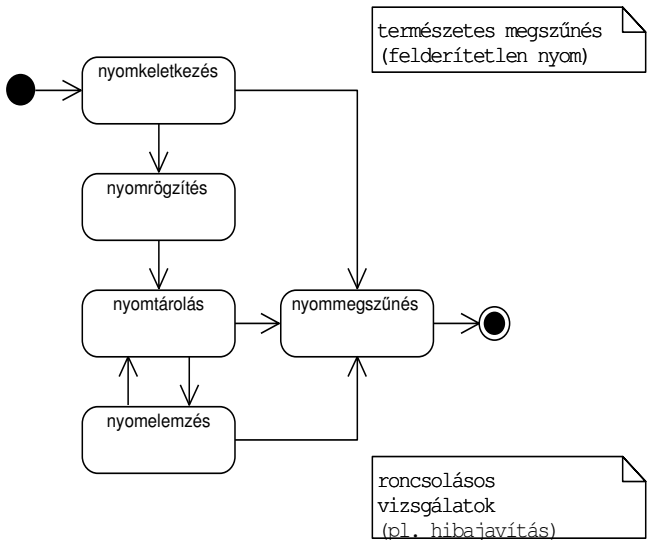
[47 pp. 29–34][4]

A hagyományos kriminalisztikában a nyomnak tág (kriminalisztikai) és szűk (traszológiai) értelmezéséről beszélhetünk, tehát:

- *„Kriminalisztikai nyom valamennyi a vizsgált ügy szempontjából releváns objektum kölcsönhatása révén keletkező anyagi jellegű elváltozás (vagyis a nyomok és az anyagmaradványok egyaránt).”*
- *„Traszológiai értelemben a nyom olyan, a vizsgált ügy szempontjából releváns objektumok kölcsönhatása révén keletkező tárgyiasult elváltozás, amely morfológiai sajátosságai révén információval szolgál a nyomképző objektumról és a nyomképződési folyamatról.”*

[48 p. 336] [4]

A nyomok általános életciklusát is modelleztem a keletkezéstől a megszűnésig, amit a következő ábra mutat be:



5. ábra – Nyomok általános állapotdiagramja (szerk.: Illési Zsolt)

Nyomok a keletkezésüket követően – a kriminalisztikus szemszögéből nézve – meg is szűnhetnek anélkül, hogy értékelésükre sor került volna, illetve az általuk a tényállással kapcsolatban hordozott információtartalmat értékelték volna. Ezek a fel nem fedezett nyomok klasszikus esetei.

Az ábra alapján kiemelt fontosságú állapot, amikor a nyomelemzés során szűnik meg a nyom. Ilyen állapotváltozásra fizikai nyomok esetében általában roncsolásos vizsgálatok során kerül sor, illetve információtechnológiai eszközök esetén például roncsolásos-szerű (az eredeti állapot módosulásával járó) változást jelent, hogy a merevlemezen található adathibák javításával elvész a hibajavítás előtti „bizonytalan", hibás állapot.

A nyomok megszűnésének a „normál" menete az, ha a nyomot felfedezik, rögzítik, elemzik, és az elemzést követően, ha a szükséges törvényi feltételek fennállnak (például az ügyet jogerősen elbírálta a bíróság), majd megsemmisítik. Amikor adatbizonyítékokról van szó, akkor az adathordozót megfelelő módon – visszaállíthatatlanul – törlik.

I.3.1.2 Daubert kritériumok

A bizonyítékgyűjtés nem lehet minden kontroll nélkül. Ha nincsenek korlátai a bizonyításnak, akkor az teret adhatna a korlátlan megfigyelésnek, az alaptalan bizonyítékok fel-

használásának – így az anyagi szabályok megkerülésével ártatlanok büntetőjogi felelősségre vonására vagy bűnösök felmentésére kerülhetne sor. A bizonyítékszerzésnek ezért jogszerűnek kell lennie, a jog által meghatározott forrásból kell származnia, illetve a Be. normáinak megfelelően kell begyűjteni, kezelni (tárolni) és értékelni.

Az egyik fontos szempont a bizonyítékok minőségének, megalapozottságának kérdése. Az egyik ilyen alapvető kontrollt az Amerikai Legfelsőbb Bíróság 1993-as a Daubert v. Merrell Dow Pharmaceuticals ügyben hozott precedens értékű ítélete jelenti a szakértők szakvéleményével (expert witness testimony) kapcsolatban. A döntés értelmében a bíróságnak ellenőriznie kell a bizonyítás során felhasznált új módszereknek a módszer által szolgáltatott bizonyíték tudományos megalapozottságát, garantálva a megfelelő alkalmazást és megbízhatóságot. Az ellenőrzés során a bíróságnak vizsgálnia kell, hogy az alkalmazott módszer

- mennyire állta ki a gyakorlat próbáját,
- hibaaránya ismert-e,
- a tudományban elismert módon publikálták-e, mi a tudományos elemzésének eredménye (megmutatható-e a hamissága, tehát falszifikálható-e, cáfolhatóság, tesztelhetőség[41]), a szakemberek közössége által elismert-e,
- keresztül ment-e alapvető gyakorlati teszteken.

[48]

A Daubert kritériumok megjelennek a szakértői vizsgálatokkal kapcsolatban a Be. 105. § (1) bekezdésében is: *„A szakértő szakértői vizsgálat alapján ad véleményt. A szakértő a vizsgálatot a tudomány állásának és a korszerű szakmai ismereteknek megfelelő eszközök, eljárások és módszerek felhasználásával köteles elvégezni."*

A Be. ezzel szemben nem említi meg a „tudományosság" kritériumát a nyomozóhatóság nyomozati feladataival kapcsolatban. Figyelembe kell venni viszont, hogy amatőr módon, megalapozatlan eljárásokkal végzett nyomrögzítés nem szerepelhet szakszerű, tudományos szakvélemény alapjául. Ezért a Daubert kritériumok betartása álláspontom szerint kötelező érvényű a nyomozóhatóságok munkájára is, az általuk végzett nyomozati munka egészére, a nyomrögzítő eljárásokra és eszközökre mind a nyílt, mind a titkos adatszerzés során. [44]

[41] L. Karl Raimund Popper osztrák és Lakatos Péter magyar tudományfilozófusok munkáit.

I.3.2 Digitális nyom

A kriminalisztikában és a traszológiában jelenleg használt nyom fogalom központjában az anyagmaradványok és a fizikai elváltozások állnak. A fizikai nyomok[42] vizsgálati módszereit a klasszikus kriminalisztika már részletesen feltárta.

A fizikai nyom és az adatmaradvány alapú szemlélet az információtechnológiai eszközök és rendszerek belső működésének vizsgálata során nem alkalmazható, hiszen a fizikai nyomokkal ellentétben a számítógépek adattáraiban, a számítógépek közötti kommunikáció során a kommunikációs csatornában nincs klasszikus értelemben vett nyom vagy anyagmaradvány; a vizsgálat során adatokat és adatmaradványokat vizsgálnak a szakértők. A hazai kriminalisztikai szakirodalomban használt nyom fogalomba azonban eddig még nem illesztették be az információtechnológiai környezet sajátosságainak megfelelő nyom ismérveit.

Jelentős mennyiségű angolszász szakirodalom foglalkozik az egyes információtechnológiai rendszerek krimináltechnikai vizsgálatával, azonban nem foglalkoznak a digitális nyommal, nem kísérelték meg definiálni azt. Ehelyett a digitális bizonyíték (digital evidence), esetenként az elektronikus bizonyíték (electronic evidence) rögzítése, felkutatása, értékelése áll az elemzéseik központjában. A digitális bizonyíték fogalma például Eoghan Casey szerint *„Digital Evidence: Encompasses any and all digital data that can establish that a crime has been committed or can provide link between a crime and its victim or a crime and its perpetrator[43].”* [50 p. 668] [44] Ez a meghatározás nem illeszkedik a hazákban általánosan elfogadott kriminalisztikai nyom fogalmához, illetve véleményem szerint nem alapozza meg a nyomfelkutatást, nyombiztosítást, nyomrögzítést. A „digitális bizonyíték” angolszász fogalma véleményem szerint már jogi értékelést is magában hordoz, hiszen a vizsgálatot végzőnek értékelnie kéne a bizonyíték büntetőjogi relevanciáját, illetve azt, hogy törvény által megengedett forrásból származik-e. Ez viszont az igazságü-

[42] Testrészek, eszközök nyomainak, az anyagmaradványok, írás/kézírás, okmány stb. vizsgálata.

[43] Digitális bizonyíték: bármilyen és minden olyan adat, ami megalapozza, hogy bűncselekmény történt, és kapcsolatot képez a bűncselekmény, annak áldozata és elkövetője között.

[44] Ehhez hasonló definíciók találhatók az internetes forrásoknál is, például:
- http://en.wikipedia.org/wiki/Digital_evidence
- http://nij.gov/topics/forensics/evidence/digital/welcome.htm
- http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/august-2011/digital-evidence

gyi szakértők esetében a kompetencia túllépéséhez vezet[45]. A „digitális bizonyíték" elnevezés és kapcsolódó fogalom azonban nem mond semmit arról sem, hogy a kriminál-technikai vizsgálatoknak mi áll a központjában, milyen nyomképző és nyomhordozó entitások vizsgálatára van szükség.

A magyar szakirodalomban találhatók utalások a „digitális nyom"-ra. Pokó István szerint *„[…] nemcsak az informatikai rendszerekben keletkező napló (log) rekordokat kell feldolgozni, hanem minden egyéb olyan adatot is, amelyekből egy adott folyamat összes lépése megbízhatóan visszakövethető, rekonstruálható. Meghatározásunk szerint ez a digitális nyom. Tehát a digitális nyom gyűjtőfogalmába, a hagyományos napló bejegyzések mellett a felhasználói rendszerek operatív adatait is beleértjük, sőt ide tartozóként határoztuk meg az egyedileg képzett – akár kézzel rögzített – adatokat, kiegészítő információkat is."* [51 p. 1]

Véleményem szerint a fenti fogalom hiányos, mivel tárgyi szempontból csak az információtechnológiai környezet hagyományos naplóbejegyzéseire, a felhasználói rendszereire korlátozódik. Az információtechnológiai infrastruktúra elemek (operációs rendszerek, számítógép-hálózatok, vállalati és egyéb hálózati adattároló rendszerek stb.) operatív adatait például nem tartalmazza.

A fogalom olyan egyedileg képzett, akár kézzel készített adatokkal, is kiegészül, amelyeket nem definiál megfelelően a szerző, így abból nem állapítható meg, hogy pontosan mit ért ezek alatt[46]. Ilyen adatok nem a nyomképződési folyamat során, hanem utána keletkeznek, így nem tekinthetők egy magatartás megítélésekor közvetlen és objektív alapnak. Nem terjed ki a fogalom a nyomképző, a nyomhordozó kapcsolódására, nincs tekintettel a nyomképződés folyamatára sem.

Pokó szerint „A digitális nyomok keresését az üzletileg kritikus folyamatok mentén érdemes végezni, ezért egy ilyen rendszer kiépítését célszerűen kockázatelemzéssel kell kezdeni. A kockázatelemzés során meghatározzuk a biztonsági és/vagy üzleti szempontból legérzékenyebb rendszereket és folyamatokat, és az ezek mentén gyűjtendő naplóadatok/operatív adatok körét, melyeket első körben javasolt bekötni a nyomelemző rendszerbe." [51 p. 1]

---

[45] L. „III. Információtechnológiai környezethez kapcsolódó kriminál-technikai tevékenységek modellezése" fejezet: a szakvélemények általános hibái.

[46] Az adatok valószínűleg a SeaLog rendszerbe bevihető, annak sajátosságaihoz igazodó (abban rögzíthető) – a publikációban sajnos nem részletezett – adatokat jelentik.

Ez a kiegészítés tovább szűkíti a digitális nyom fogalmat, mivel feleslegesen korlátozza azt az üzletileg kritikus folyamatokra. Felesleges korlátozásnak tartom a kockázatelemzés alapú szűkítést is. Sajnos az elkövetők nem aszerint válogatják meg a célpontjaikat, hogy az a sértett számára mennyire kritikus vagy kockázatos, hanem saját céljaik mentén rangsorolnak.

Egy másik szerző, Peszleg Tibor a digitális bizonyítékok alatt olyan számítástechnikai eszközről beszerzett adatokat ért, amelyeket *„bűncselekményeknél valamilyen formában számítástechnikai eszközön tároltak, feldolgoztak információkat a bűncselekménnyel kapcsolatban”*. [52 p. 25] A digitális bizonyítékokat Peszleg felosztja az alábbiak szerint:

- digitális dokumentumok,
- digitális nyomok,
- napló és regisztrációs adatok.

A digitális dokumentumokra Peszleg a következő meghatározást adja: *„egyszerű dokumentumok, könyvelési adatok, képek, videó filmek, programok, illetve bármilyen olyan adat, mely számítástechnikai eszközzel rögzíthető”*. [52 p. 25]

A digitális nyomok esetében Peszleg szerint *„általában csak időlegesen – rögzült adatokat keresünk, amelyek a számítástechnikai eszköz működése közben keletkeztek, egy átlagos felhasználó nem szerez róluk tudomást, de a rendszer működéséhez ezek az adatok elengedhetetlenül szükségesek”*. [52 p. 25]

Napló adatok alatt Peszleg olyan adatokat ért, amelyek *„egész számítástechnikai rendszerek működése és kommunikációja során keletkeznek. Ezek egy része az úgynevezett napló adatok (logok), melyek vagy törvényi kötelezettség vagy gazdasági ésszerűség, vagy rendszerbiztonsággal kapcsolatos követelmények alapján jönnek létre. Ide tartoznak a különböző szerverek fel- és letöltését naplózó adatállományok, a levelező szerverek postafiókokhoz kapcsolódó ki- és bejövő leveleket, valamint a postafiók elérését regisztráló adatállományok, de az egyes hálózatbiztonsági programok, tűzfalak, behatolás-jelző eszközök naplóadatai is.”* [52 p. 25] A regisztrációs adatok alatt a szerző olyan adatokat ért, *„melyek egy-egy szolgáltatónál keletkeznek, amikor valaki igénybe veszi szolláltatásukat”*. [52 p. 25]

A Peszleg-féle digitális dokumentum, digitális nyom, napló és regisztrációs adatlista funkcionális csoportokat jelent, melyek fogalmi egységét a büntető tényálláshoz kapcsolódás teremti meg. A felsorolás azonban nem egyenszilárdságú és nem egységes szemlé-

letű. Az értelmezési tartomány meghatározásakor a szerző csak a tárolt és feldolgozott adatokat tartja lényegesnek, nem foglalkozik a keletkező és a továbbított adatok körével, a törölt adatokat csak a digitális nyom (al)kategóriával kapcsolatban említi. Az egyes kategóriák relációja is tisztázatlan, például a digitális dokumentum fogalma annyira tág, hogy abba belefér mind a digitális bizonyíték, mind a napló és regisztrációs adat. A definíció további hiányossága, hogy nem foglalkozik az információtechnológiai környezetben a nyomképző, a nyomhordozó és a nyomképződési folyamat sajátosságaival[47].

A digitális nyom fogalmába véleményem szerint Peszleg elegyíti az átlagos felhasználó informatikai kompetenciáját, aminek semmi köze a nyomfelkutatást, -biztosítást, -rögzítést, esetleg nyomelemzést végző szakmai kompetenciájához. A digitális nyomnak a rendszer működésének elengedhetetlen feltételeként való meghatározását felesleges fogalmi szűkítésnek tartom. Mivel például a hatékonyságot szolgáló lapozófájl (swap) tartalmazhat hálózati-kapcsolati adatot, kriptográfiai kulcsokat és egyéb – egy nyomozás számára – releváns információt.

Véleményem szerint tehát a hazai digitális nyom fogalmak – az angolszász digitális bizonyítékhoz hasonlóan – nem illeszkednek a hazákban általánosan elfogadott kriminalisztikai nyom fogalmához, továbbá nem kapcsolódnak a nyomfelkutatási, nyombiztosítási, nyomrögzítési tevékenységek információtechnológiai környezetből eredő sajátosságaihoz.

Mivel a szakirodalom jelenleg még adós a megfelelő digitális nyom fogalom meghatározásával, ezért a továbbiakban áttekintem az információtechnológiai rendszerek működésének főbb jellemzőit nyomtani szempontból, és **kísérletet teszek a digitális nyom kriminalisztikai és traszológiai definiálására**.

Krimináltechnikai és traszológiai szempontból véleményem szerint kiemelt jelentőséggel bír, hogy az információtechnológiai rendszerek főleg Neumann elvű számítógépekre épülnek, amelyeknek az egyik jellemző sajátossága, hogy az operatív tárban azonos feltételek mellett tárolódnak az adatok és a programok. Az ilyen rendszerekben a rendszerprogram (operációs rendszer), az alkalmazások vagy a felhasználó kezdeményezi a műveletek végrehajtását akár az adatokon, akár a programokon.

[47] Többek között a rosszindulatú programok működésének elemzése alapján felmerül, hogy a programok végezhetnek adatkezelési műveleteket, illetve lehetnek valamely adatfeldolgozási művelet tárgyai (pl. egy megfertőzött program esetében).

Ennek a sajátosságnak a leírására a szakirodalom az információtechnológiai rendszerben lévő elemeket két csoportba sorolja:

1) **Szubjektumok** – olyan entitások a rendszeren belül, amelyek kiváltják a műveletek elvégzését, azaz: *„A TOE-n*[48] *belül többféle szubjektum is létezhet:*

a) azok, amelyek a jogosult felhasználó nevében intézkednek és szubjektumai a TSP[49] *összes szabályának*[50]*;*

b) azok, amelyek egy bizonyos funkcionális eljárásként viselkednek, viszont egy többszörös felhasználó nevében intézkednek[51]*; vagy*

c) azok, akik magának a TOE-nak a részeként intézkednek[52]*."* [53 p. 15]

2) **Objektumok** – olyan passzív entitások a rendszeren belül, amelyek információt tartalmaznak vagy fogadnak, és amelyen a szubjektumok műveleteket hajtanak végre, azaz: *„Az objektumok olyan műveletek céljai, amelyeket a szubjektumok végeznek. Abban az esetben, amikor a szubjektum (aktív entitás) lesz egy művelet célja (folyamat közötti kommunikáció), a szubjektum objektumként működhet."* [53 p. 15]

Az információtechnológiai rendszerekben a nyom keletkezésében közreműködő tényezők a kriminalisztikai és a traszológiai nyom definícióval analóg módon meghatározhatók információtechnológiai környezetben is:

- a **nyomképző**, vagyis az a szubjektum[53], amely a nyomképződési folyamat során adatokat hoz létre, továbbít, tárol, módosít vagy töröl;
- a **nyomhordozó**, vagyis az objektum[54], amelyen a nyomképző a nyomképződési folyamat során nyomot hagy;
- a **nyomképződési folyamat**, vagyis a kölcsönhatás módját meghatározó folyamat, amely meghatározza a nyom egyedi jellemzőit, fajtáját.

---

[48] TOE (Target of Evaluation) az értékelés tárgya, például operációs rendszerek, számítógép hálózatok osztott rendszerek, alkalmazások.

[49] TSP (TOE Security Policy) az értékelés tárgyára vonatkozó (biztonsági/működési) szabályok összessége.

[50] Például UNIX eljárások).

[51] Például a kliens/szerver architektúrákban található funkciók.

[52] Például bizalmi eljárások.

[53] Szubjektumnak tekinthető egy aktív funkció/program, felhasználó stb.

[54] Objektumnak tekinthetők passzív programok, adatok az operatív tárban, háttértárolón vagy valamelyik periférián.

Az információtechnológiai rendszereken belül nem értelmezhető az anyagmaradvány fogalma. A digitális nyom csak adat, vagy az adatokból kinyerhető információ lehet függetlenül az adattovábbítás és -tárolás módjától, valamint az adat megjelenési formájától.

A digitális nyom abban is különbözik a fizikai nyomoktól és anyagmaradványoktól, hogy a fizikaiaktól eltérően a digitális nyomokról (például digitálisan aláírt bitsorozat) az eredetivel megegyező másolat készíthető. A vizsgálatok korlátlan számban megismerhetők, és az azok eredménye azonos, függetlenül a vizsgálatok számától és attól, hogy az eredeti, vagy a másolt adatokon végzik el őket.

A fentiek figyelembevételével az általam javasolt digitális nyom fogalma következő:

- Kriminalisztikai értelemben: A digitális nyom olyan adat, amely a vizsgált ügy szempontjából releváns információtechnológiai rendszer szubjektumai és objektumai kölcsönhatása révén keletkezett, továbbítódott, tárolódott, módosult vagy törlődött.
- Traszológiai értelemben: A digitális nyom olyan adat, amely a vizsgált ügy szempontjából releváns információtechnológiai rendszer szubjektumai és objektumai kölcsönhatása révén keletkezett, továbbítódott, tárolt, módosult vagy törlődött, és ezáltal szolgál információval a nyomképző szubjektumról és a nyomképződési folyamatról.

[4]

I.4 Digitális nyomok rendszertana

I.4.1 Digitális nyomok általános osztályozása

A digitális nyom fogalmának meghatározása után felállítottam az információtechnológiai rendszerből kinyerhető digitális nyomok rendszertanát, amely tartalmazza ezeknek az osztályozási szempontjait az alábbiak szerint:

A digitális nyomokat csoportosítani lehet az adat (digitális nyom)

- élettartama,
- tárolási, megjelenítési helye,
- elkövetési helyhez való viszonya,
- kódoltsága, rejtettsége

szerint.

A digitális nyomok élettartam alapján lehetnek rövid, közepes vagy hosszú élettartamúak. Élettartam-sorrendre ad példát az RFC3227[55]:

- regiszter és processzorgyorsító tár,
- útvonal irányító tábla, ARP gyorsító tár, kernel statisztika, memória,
- ideiglenes fájlrendszerek,
- lemezek,
- távoli bejelentkezés és monitor adatok,
- fizikai konfiguráció, hálózati topológia,
- archív média.

[54]

A digitális nyomok tárolás, megjelenítés alapján lehetnek:

- a számítógép operatív tárjában (memóriában) található futó programok és azok adatai
- a számítógép adattároló eszközein rögzítve, ezek lehetnek:
  - a rendszer által rögzített technikai adatok, amelyek az információtechnológiai rendszer automatikus működése során jönnek létre, például:
    - temporális fájlok,
    - swap fájl/partíció,
    - információtechnológiai rendszer saját technikai adatai (munkafájlok),
    - meta- (például kép, hang EXIF) és egyéb leíró (registry, ini stb.) adatok,
    - naplóállományok – amennyiben azok alapértelmezett rendszerbeállítások mellett készülnek;
  - a felhasználó által tudatosan/akaratlagosan rögzített adatok, amelyek a felhasználó műveletei során, a felhasználó tudtával és akaratával jöttek létre, például:
    - adatbázisok,
    - adat- vagy programfájlok (például Word, Excel állományok),
    - naplók – amennyiben a felhasználónak kell aktiválnia a naplózási funkciót;

[55] Guidelines for Evidence Collection and Archiving („Irányelvek a bizonyítékok begyűjtésére és archiválására/ rögzítésére”).

- adatmaradványok, amelyek valamilyen felhasználói vagy rendszerművelet eredményeként a rendszerben megmaradnak még a művelet sikeres lefutását követően is, ilyenek:
  - törölt adatok, amelyek lehetnek
    - az operációs rendszer által menedzseltek (például MS Windows „kuka”),
    - valós törlés után az adathordozókon maradó adatok,
  - „hulladék” adatok
    - alkalmazások (például MS Word) feleslegesen/ellenőrizetlenül rögzített adatai,
    - adatállományok ideiglenes tárhelyein maradó adatok;
  - adathibák vagy adat-rendellenességek (például a támadó által szándékosan vagy véletlenül módosított adatok)
  - adathiányok (például a támadó által szándékosan vagy véletlenül törölt adatok);
- egyéb helyeken, például ha a vizsgálathoz szükséges adatokhoz
  - képernyőről,
  - hangszóróból,
  - kinyomtatott dokumentumból,
  - digitális vízjelből,
  - hálózati adatcsomagokból stb.

  lehet hozzáférni.

A digitális nyomok kódoltság, rejtettség szerint lehetnek

- nyílt adatok – az adatok az adattárolás helyének megfelelő módon vannak csak kódolva, az elemzést végző az információtechnológia során alkalmazott kódolások ismeretében tudja dekódolni azokat;
- titkosított – az adatok valamilyen szimmetrikus, vagy aszimmetrikus rejtjelzéssel kódoltak, az elemzést végzőnek nem áll a (titkos) kulcs a rendelkezésére, csak megfejtéssel tudja értelmezni az adatokat;
- szteganográfiai módszerekkel rejtett – az adatok valamilyen eljárással el vannak rejtve (például a kiterjesztés/név módosításával, vagy az üzeneteket kép- vagy hangfájl részeként való kódolásával);
- kombinált – titkosított és rejtett adatok.

A digitális nyomokat elkövetés helyéhez való viszony alapján is lehet csoportosítani, vagyis digitális nyomok találhatók:

- cél számítógép (amelyik ellen a támadás irányult),
- forrás számítógép (ahonnan a támadás indult),
- kapcsolati számítógép (amelyik valamilyen közvetítő szerepet játszik a cél és a forrás számítógép között),
- hálózati eszköz (router, switch, tűzfal stb.),
- fel- (például szerver vagy kliens számítógép) vagy kihasznált számítógép (például botnet hálózathoz tartozó „zombi”),
- (cserélhető) adathordozó.

[4] [55]

I.4.2 Digitális nyom keletkezése

Digitális nyomok taxonómiájának meghatározását követően megállapítottam a nyomok keletkezésének körülményeit is, azaz digitális nyomok keletkezhetnek:

- emberi (felhasználói) műveletek eredményeként, vagyis a támadó vagy a sértett által használt funkciók hatására (például parancsok, alkalmazások),
- automatikusan:
  - az információtechnológiai rendszer szubjektumai működésének „mellékhatásaként” (például ideiglenes fájlok, szerviz folyamatok működésének eredményei),
  - szubjektumok együttműködésének eredményeként.

A digitális és a fizikai nyom nem teljesen elkülönülten kezelendő entitások, hanem elválaszthatatlan kettőst alkotnak. Az információtechnológiai rendszerek vizsgálatakor közvetlenül nem, vagy csak speciális esetekben (például biometriai azonosítók alkalmazása esetén) lehet az egyes nyomokat természetes személyekkel összekötni. A digitális nyomok és a természetes személyek összekapcsolásakor ezért minden esetben szükséges az információtechnológiai rendszer fizikai környezetének vizsgálata anyagi nyomok és anyagmaradványok után. Azért fontos ez, hogy a digitális és a fizikai nyomképződés folyamatának zártsága erősítse a nyomozás eredményeit, és megfelelő érvrendszert szolgáltasson a bizonyításhoz és a felelősségre vonáshoz. [4]

I.4.3 Az információtechnológiai rendszerből kinyert bizonyítékok jogi értékelése

Az információtechnológiai rendszerből kinyert nyomok tehát bizonyítékforrások, és mint bizonyíték, a következő módon kategorizálhatók:

- eredeti vagy származékos,
- tárgyi jellegű,
- terhelő vagy mentő,
- közvetlen vagy közvetett (indícium).

Az eredeti környezetben működő, azaz az elkövetés idejében, az elkövetés helyén használt vagy támadott eszközöknek az infokommunikációs hálózaton továbbított adata továbbá irreverzibilis bizonyítékforrás, mivel az azon áthaladó jelek csak egyszer léteznek, csak akkor és ott (ex tunc et allicundo) vizsgálhatók.

Az információtechnológiai rendszerből kinyert bizonyítékokról megállapítható, hogy mind az elkövetés tárgyi oldaláról (in rem), mind pedig a személyi oldaláról (in personam) szolgáltat információkat.

Meg kell jegyeznem azt, hogy az információtechnológiai rendszerből bizonyíték elsősorban in rem bizonyítékforrás, csak ritkán[56] szolgáltat in personam bizonyítékokat. A felhasználói név nem azonos a felhasználóval, hiszen azonos felhasználói név alatt több személy egymástól függetlenül is tevékenykedhet. Még az sem bizonyos, hogy a jogosult felhasználó tudtával, vagy anélkül történik-e mindez. Tehát a valamilyen felhasználói név alatt elkövetett cselekmény önmagában még nem alapozza meg a felróhatóságot. Bizonyítandó, hogy a terhelt használta az adott eszközt az elkövetés idején. Ez a sajátos hangsúlyeltolódás egyébként az információtechnológiai rendszerek krimináltechnikai vizsgálatainak egészére igaz, és sajátos többlet nyomozati feladatokat generál az in rem bizonyítékok természetes személyhez kötésénél. [48] [41]

[56] Az elkövetésről készült jó minőségű online továbbított videófelvétel, vagy hálózaton keresztüli biometriai azonosításkor a küldött/fogadott biometriai adatok esetén a cselekményt végző egyedi (biológiai) sajátosságai jól azonosíthatók így az események személyhez köthetők.

I.5 Az információtechnológia sajátosságai a krimináltechnika szempontjából

I.5.2 Élő-holt rendszervizsgálat

Az információtechnológiai rendszerek vizsgálatakor lényeges szempont, hogy milyen körülmények között, milyen eszközökkel és mikor zajlik az elemzés.

A szakirodalomban elterjedt az élő-holt rendszer felosztás. Az élő rendszer eszerint a felosztás szerint azt jelenti, hogy a vizsgálatot az analizálandó számítógépen, annak operációs rendszerét és segédprogramjait felhasználva végezzük. A holt rendszer ezzel ellentétben azt jelenti, hogy a vizsgálatot saját, megbízható eszközökkel, saját, megbízható környezetben végezzük. Ez utóbbi megközelítés hatékonyabb eredményt szolgáltat ugyan, de sajnos nem mindig megvalósítható a gyakorlati életben (például egyedi eszközök és prototípusok vizsgálatánál, speciális vizsgálati környezet és segédeszköz hiányában, továbbá, ha nagyon gyors, azonnali helyszíni elemzésre van szükség).

A számítógép-hálózatok krimináltechnikai szakirodalma ezzel szemben nem ilyen módon osztja fel a feladatokat, hanem a számítógép-hálózatokból kinyerhető adatforrások alapján írja le a folyamatot:

- hálózati komponensek azonosítása,
- ISO/OSI modell vizsgálata,
- együttműködés rejtett hálózati ügynökökkel és a szerverek kontrollja,
- hálózati adatok (forgalom) mentése,
- hálózati adattárolók keresése,
- folyamatok újraalkotása a forgalom alapján.

[56 pp. 241–263]

A másik megoldás a számítógép-hálózatok IP protokoll vagy ISO/OSI rétegalapú megközelítése. [50 pp. 370–380]

A gyakorlati tapasztalatok alapján úgy vélem, hogy az élő-holt megközelítés kiegészítésre szorul, mert nincs tekintettel az elkövetés és az elemzés időbeni kapcsolatára (egyidejű vagy követő vizsgálat), illetve nem eléggé pontosan határolja el a vizsgált eszköznek és környezetnek az analízisre gyakorolt befolyását. A fenti felosztások közül a második a krimináltechnikai vizsgálatok leírására nem alkalmas, mert fókuszában csak a hálózati rétegek állnak, a bizonyítékok megszerzésének módjáról és időzítéséről nem szól. A

fentiekre tekintettel egy olyan megközelítést javaslok, amely az élő-holt felosztáshoz hasonlít leginkább, de tovább finomítja azt az alábbiak szerint:

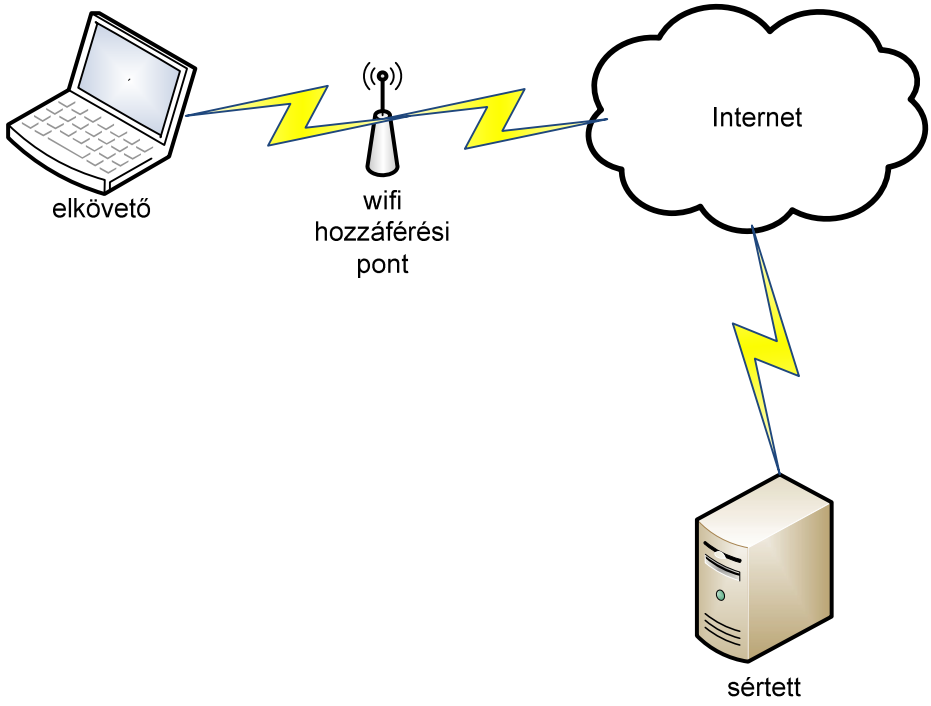
- az elkövetés-vizsgálat időbelisége alapján:
  - az elkövetéssel egyidejű,
  - az elkövetés után végzett;
- vizsgált rendszer működési állapota alapján:
  - kikapcsolt (holt),
  - bekapcsolt (élő);
- a vizsgálóeszköz (program) kontrollja alapján:
  - a vizsgált rendszerbe integrált (a vizsgált rendszer kontrollja alatt álló),
  - a vizsgált rendszertől független (a vizsgált rendszernek nincs kontrollja a vizsgálóeszköz felett).

I.5.3 Számítógép-hálózatok vizsgálata

Amennyiben egy számítógép-hálózat része egy információtechnológiai – illetve az azzal összefüggő – bűncselekmény valódi vagy virtuális helyszínének, vizsgálni kell, hogy:

- Hogyan lehet egy számítógép-hálózathoz kapcsolódni?
- Honnan lehet a számítógép-hálózathoz kapcsolódni?
- Milyen bizonyítékértéke van a számítógép-hálózatból szerzett információnak?

A számítógép-hálózatot is tartalmazó bűncselekmény helyszínének egy lehetséges vázlata egy hekkertámadás esetén a következő lehet:



6. ábra – Számítógép-hálózatot is érintő bűncselekmény egy lehetséges elvi vázlata (szerk.: Illési Zsolt)

Ilyenkor a kommunikáció során a résztvevő eszközözök az egyedi hardver azonosítót (MAC cím) vagy a hálózati kommunikációban használt egyedi-logikai azonosítót (IP cím) használják fel a kapcsolat kiépítésére és fenntartására.

A mérés során az okozhat gondot, hogy a MAC cím csak a következő útválasztóig (router) azonosítja a számítógépet, ezután ethernet hálózatok esetén az adatot továbbító útválasztó MAC címe azonosítja a csomagot a következő útválasztóig. A MAC címet egy közepesen képzett, informatikában alig járatos felhasználó is képes megváltoztatni megfelelő segédprogramok segítségével, amelyekből jó néhány található meg egy gyors Google kereséssel. Ezek alapján látható, hogy a hálózati forgalomban található MAC cím nem, vagy csak egy-egy szegmensen használható fel egy munkaállomás azonosítására, és az azonosítás csak addig érvényes, amíg a felhasználó meg nem változtatja azt.

Egyes (speciális) esetekben előfordulhat, hogy a forrás számítógép MAC címe túlél egy-egy kommunikációs csomópontközi ugrást (például a MS Word által készítet dokumentumokban tárolt egyedi azonosítókban) – így felhasználható az azonosításra.

A forrás IP címe már egy kicsit több információval szolgálhat, hiszen egy felépített TCP/IP kapcsolat alapfeltétele, hogy az IP cím a kommunikációs csatorna végeit egyértelműen azonosítsa.

A probléma a kapcsolat-felépítési és -bontási csomagokkal van, hiszen ezek lehetnek hamisított (ún. spoof-olt) címek, amelyeknek semmi közük nincs az elkövető számítógépének valós IP címéhez[57]. A hamisított UDP alapú kommunikációnál – amennyiben az elkövető csak egy irányban használja a csatornát – szintén nem használható fel a kommunikációban szereplő IP címe.

Az IP címek felhasználhatóságának korlátja még az esetleges virtuális magáncsatornák alkalmazása, amikor az elkövető egy titkosított csatornán át, esetleg több számítógépen keresztül (például proxy, onion routing) éri el a sértett számítógépét. Ilyen esetben csak a titkosított csatorna két szélén lévő határtitkosító állomások és a sértett számítógépe (a támadás vagy elkövetés célja), illetve az elkövetésre felhasznált számítógépe között nyerhető ki az adatforgalomból.

Az elkövetésre felhasznált számítógépnél tehát az adatcsomagok az elkövető számítógép azonosságához nyújtanak információkat. A sértett számítógépének oldalán pedig inkább a támadás jellegére, az elkövetett bűncselekményre utaló adatokat szolgáltat az adatforgalom.

Meg kell azonban jegyezni, hogy a számítógép-hálózatok elemzéséből származó adatok nem, vagy csak nagyon közvetve szolgáltatnak az elkövető kilétére irányuló (személyi vonatkozású) adatokat, mivel a vizsgálatok technikai jellege miatt „megáll” az elkövetésre felhasznált eszköznél. Az elkövetési eszköz azonosítása után további nyomozási cselekményekre van szükség, hogy az elkövetés tárgyát összekösse az elkövető személyével (például ujjlenyomat vétele a billentyűzetről, videó vagy egyéb felvétel az elkövetés közben, az elkövető vallomása stb.).

Számítógép-hálózatok esetén lényeges szempont továbbá az, hogy egy-egy csomag csak milliszekundumokig „él”, valamint vezeték nélküli technológiára épülő hálózat esetén csak az általa lefedett területen fogható.

A vezeték nélküli hálózatok sajátossága a vezetékes hálózatokkal ellentétben, hogy a hálózathoz kapcsolódó végpontok térereje a kapcsolat ideje alatt végig mérhető, így adatot szolgáltat arról, hogy a kommunikáció során mely más – a vezeték nélküli hálózaton

[57] Hamisított címeket elsősorban túlterheléses jellegű támadásokra lehet felhasználni, ilyenek használatával azonban nehéz, majdnem lehetetlen működő TCP kapcsolatot létrehozni és fenntartani.

belüli – végpontokkal kommunikálhat. Továbbá kisugárzás esetén megfelelő antennákkal és mérővevőkkel az irány is meghatározható (adóteljesítmény ismeretében a távolság is).

A számítógép-hálózathoz való kapcsolódást a fizikai jelek mellett adatmaradványok (digitális nyomok) is megőrzik. Ilyen nyomokat őrizhet:

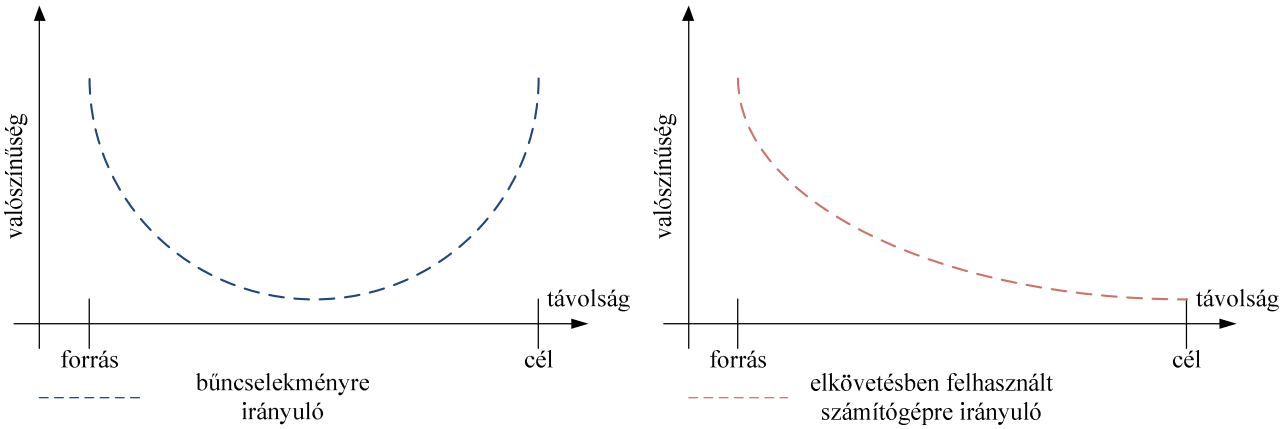
- a forrás számítógép,
- a sértett számítógépe (cél),
- a kommunikációban résztvevő valamennyi eszköz[58]

a memóriájában, naplóállományaiban stb.

A fentiekből következik tehát, hogy a számítógép-hálózat elemzéséből kinyerhető bizonyítékok

- bizonyító ereje (az esemény valószínűségét megerősítő volta) és
- típusa[59]

összefüggésben vannak az adatszerzésnek a forrástól vagy a céltól való távolságával. Ezt a viszonyt a 7. ábra szemlélteti.



7. ábra – Számítógép-hálózatból kinyerhető bizonyítékok bizonyító ereje, típusa a forrástól és a céltól való távolság függvényében (szerk.: Illési Zsolt)

[58] A kapcsolódáshoz használt kapcsoló (switch), WiFi végpont, továbbá a kommunikációban résztvevő útválasztók, tűzfalak stb.

[59] A bizonyíték típusa lehet
- személyi vonatkozású, vagyis az elkövetésben felhasznált eszközzel kapcsolatos, vagy
- tárgyi vonatkozású, vagyis a bűncselekményre irányuló, azzal kapcsolatos

gyanút növelő/csökkentő tényező.

A Wifi hálózatoknak a vezetékestől eltérő sajátossága, hogy bárki csatlakozhat hozzá – egyes esetekben akár véletlenül is –, tehát az ilyen nyílt hálózatokhoz kapcsolódó vizsgálatok elvégzésekor mindig vélelmezni kell, hogy a hálózati forgalmat nemcsak a jogosult felhasználók generálták, bárki kívülről is lehetett az adó/vevő.

A gyakorlatban a WEP kódolású hálózat védelme egy perc alatt törhető[60]; a számítógép-hálózat egyéb védelmi mechanizmusai, mint a MAC címszűrés, a hálózati azonosító (Service Set Identifier, röviden: SSID) sugárzásának tiltása hatástalan. A SSID-t a hálózati forgalom lehallgatásával meg lehet ismerni[61], a MAC cím pedig klónozással egyszerűen megváltoztatható a hálózatban aktívan kommunikáló számítógépek MAC címeinek ismeretében. Ezek alapján kijelenthető, hogy a WEP kódolással védett számítógép-hálózatok viszonylag alacsony informatikai felkészültségű elkövető számára is eredményesen támadhatók, ezért vélelmezni lehet, hogy az ilyen hálózatokba nemcsak a hálózat rendszergazdája/üzemeltetője által engedélyezett felhasználók kapcsolódhatnak.

A WPA és a WPA2-es kriptográfiai védelmet alkalmazó WiFi hálózatokat biztonságosnak lehet mondani, amennyiben az alkalmazott kulcsméret elegendően nagy[62] és az alkalmazott kulcs entrópiája[63] magas. A biztonságos WPA és WPA2 hálózatoknál – az ellenkező bizonyításáig – azt kell feltételezni, hogy a hálózatot csak a rendszergazda által feljogosított számítógépek és felhasználók használták.

Egy 2007-es felmérés szerint Budapest belvárosában egy statisztikai elemzésre alkalmasan választott minta alapján a hálózatok:

- 42%-a védelem nélküli,
- 31%-a WEP kódolású,
- 27%-a WPA vagy WPA2 titkosítással védett.

[57]

A fenti adatokból egyértelműen kiviláglik, hogy amennyiben egy bűncselekmény elkövetése során számítógép-hálózati elem is része a bűncselekmény fizikai vagy virtuális hely-

[60] L. http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack

[61] A 802.11-es szabvány szerint a hozzáférési végpontok időközönként mindeknek szóló (broadcast) üzenetekben (ún. „Bacon csomagok") hirdetik az eszköz adatkapcsolati képességeit. Ezeknek a csomagoknak fejlécében nyílt formában megtalálható az SSID.

[62] Nagyobb, mint 16 karakter.

[63] Azaz: az alkalmazott jelkészlet véletlenszerűsége nagy, esetleg nem szabályszerűen képzett (pl. sorszám), nem található meg szótárakban.

színének, úgy a végpont karakterisztikája, az alkalmazott kódolás típusa az ügy szempontjából releváns, és ezeket a jellemzőket a nyomozás során érdemben vizsgálni kell. [58]

I.5.4 „Nyílt" vs. „zárt" rendszerek használata az igazságügyi szakértés során

I.5.4.1 „Zárt" rendszerek (kereskedelmi szoftverek)

A számítógépek megjelenésével szinte egyidősek a kereskedelmi szoftverek. Az információtechnológiai őskorára ez a fejlesztési modell a jellemző.

A zárt fejlesztői világ anyagi haszonszerzés végett fejleszti a termékeit, ezért a fejlesztők fókuszában a fizetőképes keresletet megtestesítő fogyasztók, illetve azok elvárásai állnak. A zárt rendszerek megalkotói a programjaikat jogi és technikai intézkedésekkel védik a visszafejtéstől, hiszen a szoftverben megtestesülő újítások képezik a gazdasági haszonszerzés alapjait.

A fejlesztő, gyártó cég a marketing eszközeivel méri fel a piac igényeit, fogalmazza meg a termék fejlesztésének értékesítésének stratégiáit és csatornáit, illetve ha kell, a marketingkommunikáció eszközeivel növeli a termék jó hírét, és csökkenti a problémák következményeit. Az ilyen marketingkommunikációra jellemző példa a Microsoft azon törekvése, hogy lejárassa az ellenfeleit[64], a programok hibáinak letagadása[65], a VISTA operációs rendszer körüli hiábavaló felhajtás, vagy az XP operációs rendszer előre nem tervezett hosszúságú életciklusa.

A szabad szoftverek megjelenésével egy időben a „zárt" szoftverek fejlesztői is keresik azokat a megoldásokat, amellyel kezelni tudják a szabad szoftverek elterjedésének következményeit. Ennek egyik példája a Microsoft által folytatott FUD[66] kampány, a másik – a felhasználók számára hasznosabb megoldás – a kereskedelmi szoftverek kisebb

[64] Válaszul az Apple cég „I'm a Mac" kampányára, vagy a Linux és az open source előretörésére.

[65] A CVE-2008-5745 referenciájú Media Player buffer túlcsordulásos támadásról és lehetséges következményeiről a Microsoft nem adott kielégítő információt, továbbá a sebezhetőség hatását a valóságosnál lényegesen kisebbként mutatta be.

[66] Fear, Uncertainty, and Doubt.

tudású, de ingyenes verzióinak a piacra dobása[67], vagy a szoftverek köré épített szolgáltatások körének bővítése[68]. [59]

I.5.4.2 „Nyílt" rendszerek (szabad/nyílt forráskódú szoftverek)

Bár a kereskedelmi szoftvernek fogalmilag nem ellentéte a szabad, vagy nyílt forráskódú szoftver, de a téma szempontjából e két fejlesztési/terjesztési modell a mérvadó. A következőkben ismertetem a „nyílt" projektek eredményeként megszülető szabad és nyílt forráskódú projekteket és azok jellemzőit.

Az információtechnológia fejlődésével, a gazdasági haszon növekedésével párhuzamosan a gazdasági szervezetek rutinszerűen kezdték el alkalmazni a felhasználókat, a programozókat korlátozó licencszerződéseket. A fejlesztők közössége – főleg az akadémia szektorban[69], de az egyes gyártók eszközei köré csoportosuló felhasználói közösségek[70] – ezzel párhuzamosan elkezdte hangsúlyozni, hogy az általuk fejlesztett szoftver nem árucikk, hanem olyan közkincs, amelynek szabad felhasználása a társadalom érdeke. Vizsgálhatósága, kutathatósága hasznos az oktatás számára, a tudomány és a technológiai fejlődés motorja lehet.

A gazdasági szervezetek szerződéseinek mintegy jogi ellenlábasaként 1983-ban Richard M. Stallman, a szabad szoftver mozgalom atyja, a GNU[71] projekt keretében megalkotta az első olyan szoftver licenciát, amely a szerzőnek csak a személyhez fűződő jogait védi – jórészt szerzői névfeltüntetés formájában. Ugyanakkor a felhasználási, továbbfejlesztési tilalmak és korlátozások helyett a szerző vagyoni jogát korlátozza, de lehetőséget ad a szoftver szabad felhasználására, továbbfejlesztésére[72].

A szabad szoftver mozgalom nemcsak a jog mezején vetélytársa a kereskedelmi szoftvereknek, de lassan a megbízhatóság, használhatóság és választék terén is felveszi a versenyt a „zárt" szoftverrel. A Linux szerverek elterjedése, vagy a Mozilla Firefox web-

---

[67] Például a Grisoft cég AVG free antivírus szoftvere.

[68] Például az Ubuntu Linux disztribúciót támogató dél-afrikai Canonical által nyújtott oktatási, technikai támogatási szolgáltatások.

[69] Többek között a Massachusetts Institute of Technology (MIT) is jelentős mennyiségű nyílt forráskódú szoftvert bocsát a felhasználók rendelkezésére.

[70] Például az IBM 701 SHARE vagy a DEC DECUS felhasználói csoportjai.

[71] A GNU az FSF (Free Software) alapítvány által GNU IS NOT UNIX (GNU NEM UNIX) rekurzív rövidítéssel jelölt projekt, amelynek célja egy Unix-szerű szabad szoftver fejlesztése.

[72] L. http://en.wikipedia.org/wiki/Open_source

böngésző folyamatos előretörése is jelzi, hogy a nyílt forráskódú szoftverek piaca folyamatosan tágul a kereskedelmi szoftverek elterjedésének rovására. [59]

I.5.4.3 Nyílt és zárt rendszerek összehasonlítása

Az alábbiakban a nyílt és zárt forráskódú forenzikus rendszereket hasonlítom össze informatikai igazságügyi szakértői szempontból:

Szempont	**Zárt rendszerek**	**Nyílt rendszerek**
Daubert 1: gyakorlati próba	▪ bíróságokon többször (sikerrel) megméretett	▪ bíróságokon többször (sikerrel) megméretett
Daubert 2: ismert hibaarány	▪ hibák marketingje ismert, a gyártó/fejlesztő elemi érdeke a hibákkal kapcsolatos információk „kordában tartása”	▪ hibái ismertek, a közösség számára adott a lehetőség valamennyi feltárt hiba (és javítás) megismerésére
Daubert 3: publikált-e, elemzésének eredménye a szakemberek közössége által elismert-e	▪ főleg a gyártó/fejlesztő által preferált forrásokban és módon publikált ▪ forráskód nem megismerhető (fekete doboz) ▪ az elemzések eredményét a gyártó/fejlesztő igyekszik kontrollálni ▪ főleg a fejlesztő cég és a vásárlói közösség által elismert	▪ az interneten szokásos módon publikált ▪ forráskód szinten megismerhető (fehér doboz) ▪ az elemzések eredménye publikus ▪ fejlesztői/felhasználói közösség által elismert
Daubert 4: keresztül ment-e alapvető gyakorlati teszteken	▪ a gyártó/fejlesztő által tesztelt, az új verziókat is a gyártó/fejlesztő fogadja el ▪ kereskedelmi igény esetén biztonsági (ISO14508) szerint tanúsított termék	▪ a fejlesztés során a közösség teszteli és fogadja el az új verziókat, a széttagolt fejlesztői és felhasználói csoportok miatt rendszerint komoly tesztelést követően ▪ általában (fejlesztői forráshiány miatt) a terméknek nincs tanúsítványa

Szempont	Zárt rendszerek	Nyílt rendszerek
Fejlesztés	▪ kereskedelmi igény esetén a gyártás ISO 9000-szerint tanúsított ▪ a fejlesztő eszközök nem vagy csak korlátozott mértékben ismertek ▪ a fejlesztő többnyire zárt (általa sem teljes egészében ismert, teljesen dokumentált) kereskedelmi fejlesztőeszközökkel fejleszt	▪ a fejlesztési folyamat nyílt, de főként nem tanúsított ▪ a fejlesztő eszközök teljes körben ismertek ▪ nyílt forráskódú fejlesztőeszközök felhasználásával készül
Módosíthatóság	▪ a forráskód jogi és technikai eszközökkel védett, legálisan nem módosítható	▪ forráskód/funkció szabadon módosítható
Ki- és bemeneti formátum	▪ sok esetben jogvédett, technikai korlátos kimeneti formátum	▪ szabványos formátumok
Lekérdezési, feldolgozási lehetőségek	▪ sok esetben jogvédett beépített programspecifikus lekérdezési módszerek	▪ szabványos reguláris kifejezések ▪ program-csővezeték (pipeline)
Funkcionalitás teljes körűsége	▪ funkciók ~zártak (egy-egy problémakörre)	▪ funkciók töredékesek, esetleg hiányosak, rendszerint csak több program együttműködésével oldható meg
Kezelhetőség	▪ valamennyi funkció integrált grafikus felületen keresztül érhető el, egyszerű kezelhetőség[73]	▪ integrálatlan grafikus és karakteres felület, bonyolult kezelhetőség[74]
Fejlesztői támogatás, fejlesztés stabilitása	▪ fejlesztés a fizetőképes piaci kereslettől függ	▪ fejlesztés esetleges (de rendszerint stabil)

[73] A programok többnyire grafikus felület és „bolond biztos” beállítások és egyszerűsítések mögé rejtik a feladat komplexitását. A kezelőnek közepes informatikai ismeretekre, esetleg programspecifikus tanfolyami végzettségre van szüksége a működtetéshez és a kimeneti adatok értelmezéséhez.

[74] A programok nagymértékben paraméterezhetők, a funkciói esetenként grafikus és karakteres felületen is elérhetők. A felhasználónak nemcsak az alkalmazott technológiákat, de a technológiai környezet paramétereit is ismernie kell a kezeléshez. A vizsgálatot végzőnek nagy szakismeretre van szüksége a programok kezeléséhez és az eredmények értelmezéséhez.

Szempont	Zárt rendszerek	Nyílt rendszerek
Vizsgálatok eredményei technikai sebezhetőségein keresztül manipulálhatók (érzékenység anti-forensic támadásokra)	▪ egyedi (az eszköz adatfeldolgozási vagy egyéb sérülékenységeire épülő) technikákkal támadható	▪ egyedi (az eszköz adatfeldolgozási vagy egyéb sérülékenységeire épülő) technikákkal támadható

1. táblázat – Nyílt és zárt forenzikus rendszerek összehasonlítása (szerk.: Illési Zsolt)

[59]

A nyílt és zárt rendszereket összehasonlító táblázatból kitűnik, hogy a zárt rendszerek nem felelnek meg maradéktalanul a Daubert kritériumoknak[75], ezért azok alkalmazhatósága megkérdőjelezhető.

Sajnos, értekezésem megírásának idején a forenzikus vizsgálatokhoz használt eszközök szisztematikus összehasonlítása nem áll rendelkezésre, de nem készült el eddig a piacon fellelhető valamennyi zárt és nyílt forenzikus funkciókat támogató hardver és szoftver eszköz katalógusa sem. A katalógus elérhetetlensége mellett a tudományos igényességű összehasonlítás gátja a zárt rendszerek ára is. Ma hazánkban nincs olyan forenzikus labor, ahol ezeknek a termékeknek a többsége, de legalább azok az eszközök rendelkezésre állnának, amelyekkel a vizsgálatok 80%-át elvégzik[76,77].

A zárt rendszerek számára jelentős előnyt jelent az, hogy velük a vizsgálatokat a szakértők lényegesen hamarabb és sokkal kényelmesebben tudják elvégezni. Továbbá ezek a rendszerek olyan komoly tudásbázisra építik a működésüket, hogy a felhasználónak sokszor nem is kell mély ismeretekkel rendelkeznie a vizsgált adatstruktúrákról (például a

[75] A nem-megfelelőség oka az ismeretlen hibaarány; korlátozottan publikált működés; „zárt” forráskód, „zárt” hardver; a gyártó által felkért, kérdéses függetlenségű tesztelés.

[76] A szakmai közösségek kialakulását nehezíti a szakértői tevékenységek individualizációja Magyarországon. Ezt mi sem bizonyítja jobban, mint az, hogy 2012. augusztus 30-án a Minisztérium igazságügyi szakértői nyilvántartása szerint informatikai kompetenciával összesen csak két szakértői intézet, az Igazságügyi Szakértői és Kutató Intézet (2 fő) és a Bűnügyi Szakértői és Kutatóintézet (1[?] fő) rendelkezik. Ezzel szemben 25 igazságügyi szakértői cég profiljában szerepel az informatika mint kompetencia, azonban ezek közül 13-nak csak 1 igazságügyi szakértő tagja van, 5-nek pedig 2. Ilyen kis laboroknak pedig egy-egy szűk feladatkörre épülő eszközpark beszerzése is komoly költséget jelent.

[77] Nincs tudomásom olyan informatikai forenzikus laborról hazánkon kívül sem, ahol ezek a hardver és szoftver eszközök rendelkezésre állnának, és az összehasonlító vizsgálatokat el tudnák végezni.

Windows Registry adatbázisának vagy naplófájljainak struktúrájáról, vagy az NTFS fájlrendszer `$MFT` fájljának struktúrájáról). A program automatikusan feldolgozza ezeket, és „konyhakészen" tálalja az eredményeket. A nyílt rendszerek ezzel szemben nem rendelkeznek kiterjedt és integrált tudásbázissal, minden lényeges adatot, kapcsolatot a vizsgálatot végző szakértőnek kell ismernie. Ezért a nyílt rendszerekkel végzett vizsgálatokhoz szükséges szakértelem esetenként lényegesen nagyobb lehet a zárt rendszerekéhez képest[78]. A hatóságok és a büntetőeljárás többi résztvevőinek az az igénye azonban, hogy a szakértő minél hamarabb végezze el a vizsgálatot, olyan erős, hogy valamennyi lényeges szereplő törekszik a zárt rendszerek beszerzésére és alkalmazására.

Meg kell jegyeznem azonban azt is, hogy a zárt rendszerek már többször is kiállták a tárgyalóterem próbáját, továbbá több büntető és polgári perben is elfogadta a bíróság az ezekből származó bizonyítékokat, és ezekre alapozva hozta meg döntéseit. Azonban ez a gyakorlati próba nem jelenti azt, hogy ne lenne szükség a zárt rendszerek tudományos alaposságú publikációjára, az elsőfajú[79] és másodfajú[80] hibaarány megbízható tesztelésére.

I.5.4.4 „Nyílt forráskódú" vizsgálati módszerek

Az informatikai igazságügyi vizsgálatoknak nemcsak a szoftverek a lényeges kellékei. Szükséges még, a szakértő úgy végezze el az analízist, hogy az megfeleljen a jogszabályi előírásoknak és a szakma szabályainak.

E két elvárás közül a jogszabályi tűnik egyszerűbbnek, mivel az információtechnológia fejlődése (a Moore-törvénnyel[81] összhangban) exponenciálisan nő, az egyre olcsóbb eszközökön egyre nagyobb komplexitású szoftverrendszerek futnak, és ezáltal folyamatosan nő a tudományterülethez tartozó szabványok, ajánlások, módszerek köre, amelyben egyre nehezebb eligazodni.

Az informatikai igazságügyi szakértést szakmai módszertanok, eljárási segédletek is támogatják. Ezek közé tartozik – egyfajta szakmai minimumnak számít – az amerikai

[78] A probléma analóg a gépi kódú és a 4GL eszközökkel történő fejlesztéssel.

[79] Vaklárma, vagy fals pozitív hiba.

[80] A keresendő értéknek megfelelő, de nem azonosított érték, azaz fals negatív hiba.

[81] Gordon E. Moore 1965-ös publikációjában írta le először, hogy az egységnyi felületre integrálható tranzisztorok száma exponenciálisan nő, körülbelül minden második évben megduplázódik a számuk. Moore törvényéről azóta kiderült, hogy ez a megállapítás az információtechnológia szinte minden területére igaz: a feldolgozási sebességre, a memória kapacitásra, még a digitális kamerák felbontására (a pixelméret csökkenésére és a pixelek darabszámának növekedésére) is.

igazságügyi minisztérium 2004 áprilisában kiadott ajánlása, amely iránymutatást ad arra vonatkozóan, hogy a számítógéppel kapcsolatos ügyekben hogyan kell:

- a bizonyítékokat értékelni,
- a bizonyítékokat begyűjteni,
- a bizonyítékokat vizsgálni,
- dokumentálni az eredményeket.

Az ajánlás tartalmaz még további információkat a szakértéssel kapcsolatban, minta esettanulmányt, munkalapokat, jogi, technikai és szervezeti erőforrások listáját stb. [60]

Az internet, mint minden számítástechnikával kapcsolatos instrumentum, szabványos alapokra épül. Az internet sajátos szabványait RFC-nek (Request For Comments) nevezik, és ilyenek írják le a lényegi működési protokollokat, technológiákat. Az igazságügyi szakértői vizsgálatoknak is van ilyen szabványa a 3227-es, a Guidelines for Evidence Collection and Archiving (*„Irányelvek a bizonyítékok begyűjtésére és archiválására/rögzítésére”*).

Az RFC meghatározza, hogy biztonsági események esetén – általában az információtechnológiai környezetben elkövetett bűncselekmények elkövetésekor is – mit és hogyan kell tenni annak érdekében, hogy minden nyom megmaradjon, vagyis hogyan kell begyűjteni, és miként kell archiválni, rögzíteni.

Az RFC 3227 négy fejezetből áll:

1) Iránymutató elvek a bizonyítékok begyűjtésekor
2) Bizonyíték begyűjtési eljárás
3) Bizonyíték archiválási eljárás
4) Szükséges eszközök

[54]

Az internetes közösség ezek mellett további módszereket is kidolgozott. Ilyen például a Sourceforge.net-en található Open Source Computer Forensics Manual (2003.07.15) – amelynek fejlesztése látszólag ugyan időközben leállt, azonban a valóság az, hogy a fejlesztések csak átmentek az http://www.opensourceforensics.org/ oldalra. Itt nemcsak módszertan érhető el, hanem megtalálhatók egyéb, idevágó:

- Windows és Linux környezetben alkalmazható eszközök,
- eljárások,
- tesztek/példák,
- kutatási dokumentumok.

Meg kell említenem azt is, hogy vannak olyan igazságügyi szakértésre, biztonsági vizsgálatokra szakosodott Linux disztribúciók is, amelyek már jelenlegi formájukban is alkalmasak az igazságügyi szakértői munka támogatására. Ezek közül kiemelkedik a HELIX 3, amely egy folyamatos fejlesztés során 2008 szeptemberében kiadott nyílt forráskód-alapú rendszer. A HELIX3 egy LIVE CD-re telepített Windows és Linux operációs rendszerkörnyezetben is alkalmazható segédprogram-gyűjtemény és -dokumentáció. [59] [61]

Következtetések

Az információtechnológiai környezetben elkövetett támadások és bűncselekmények elemzésekor **megállapítottam, hogy az információtechnológiai környezetben elkövetett bűncselekmény fogalma tágabb, mint a számítógép-hálózati támadás fogalma**. Bűncselekmények esetében a védett érték nemcsak közvetlenül az információtechnológia, hanem minden, a társadalomra veszélyes magatartás, amelyben a technológiát felhasználták, vagy amelyeknek ilyen eszközök a tanúi. Minden bűncselekménynek lehet információtechnológiai vetülete, amelyet az informatikai igazságügyi szakértő érdemben vizsgálhat. **Megállapítottam** továbbá, **hogy** az információtechnológiai környezetben **a támadások** a fegyveres összetűzések joga alapján **elkövethetők jogszerűen, illetve jogellenesen**, az ebben a környezetben elkövetett **bűncselekmények viszont minden esetben jogellenesek**. Krimináltechnikai jelentősége viszont csak a törvény által büntetni rendelt magatartásoknak, illetve az ezekkel összefüggő nyomokat tartalmazó technológiai rendszereknek és eszközöknek van.

Megállapítottam, hogy a kriminalisztikában jelenleg alkalmazott nyom fogalma **csupán a** bizonyítékként felhasználható indíciumok **fizikai megjelenítési formá**já**ra összpontosít, nem veszi figyelembe a virtuális térben felhalmozódó bizonyítékforrások sajátosságait**.

Az adatmaradványok természete csak lazán kapcsolódik a fizikai világhoz. Digitális bizonyítékok egy időben több helyen is képződhetnek, eltérő adattárolókban, eltérő fizikai közegben lehetnek eredeti, vagy az eredetitől meg nem különböztethető formában jelen. A jelenleg használt nyom fogalom többek között nem veszi figyelembe az információtechnológiai rendszerekben képződő, bizonyítékként felhasználható nyomok ezen sajátosságait. Ezért **megalkottam a digitális nyom fogalmát, összhangban a jelenleg használatos anyagmaradvány és lenyomat** központú traszológiai és kriminalisztikai **nyom fogalommal**.

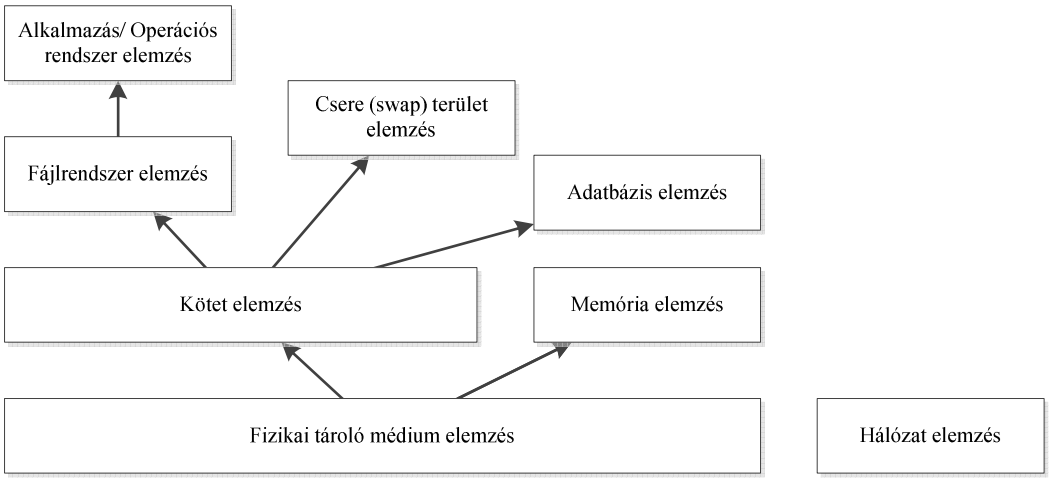
A digitális nyom definiálását követően meghatároztam annak csoportosítási jellemzőit, keletkezési körülményeit, bizonyítékként való felhasználásának jogi szempontú osztályait, ezzel létrehoztam a digitális nyomok taxonómiáját.

Az információtechnológia sajátosságainak figyelembevételével meghatároztam azokat a sajátosságokat, amelyek nem jellemzők az egyéb (fizikai) nyomokra, illetve az egyéb nyomok vizsgálatakor felhasznált módszerekre.

Az információtechnológiai törvényszéki vizsgálatoknál használt eszközökkel kapcsolatban megmutattam, hogy azok nem felelnek meg maradéktalanul a Daubert kritériumoknak, az eredmények tudományos értéke sérül, mert a széles körben alkalmazott forenzikus hardverek és szoftverek zártak, nem ismerhető meg működésük minden részlete.

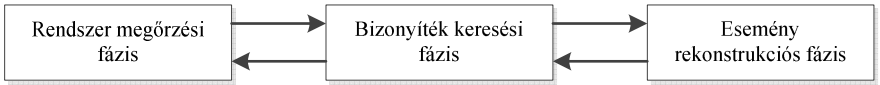
II. INFORMÁCIÓTECHNOLÓGIAI RENDSZEREK KRIMINÁLTECHNIKAI VIZSGÁLATÁNAK RÉTEGMODELLJE

Brian Carrier 2003-ban publikált egy réteg-megközelítést, amelyet az adathordozók vizsgálatának elemzéséhez használt. [62] Az ő eredeti réteg-megközelítése a számítógép-hálózatokra közvetlenül a rétegmodellbe nem illeszkedő, attól eltérő entitásokra tekint. A modell alapján látható, hogy az egyes elemzési lépések fastruktúrában kapcsolódnak egymáshoz, az egyes levélelemek között azonban nincs közvetlen elemzési kapcsolat, a fájlrendszer és alkalmazás/operációs rendszer elemzését nem köti össze az adatcsere (swap) területek, az adatbázisok és a memória elemzésével. Ezt a modellt egy későbbi publikációjában grafikusan is ábrázolta a 8. ábra szerint.



8. ábra – Elemzési rétegek – a digitális adat felépítése alapján (Forrás: [63 p. 11])

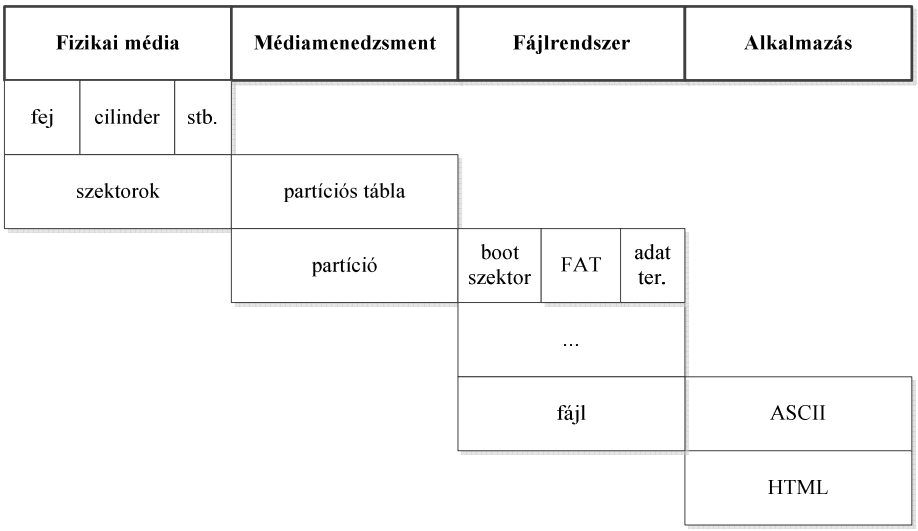
Az eredeti modell-megközelítés közvetlenül nem tartalmazza az egyes rétegek közti vizsgálatok visszacsatolásának lehetőségét. A lehetséges visszacsatolásokat a 9. ábrán látható módon Carrier külön, a forenzikus munkafázisok alapján képzeli el:



9. ábra – A digitális bűncselemény helyszín vizsgálatának három fő fázisa (Forrás: [63 p. 5])

A modellben az egyes absztrakciós rétegeket röviden kifejti – a leírásokat én is ismertetem az egyes rétegek leírásakor –, és felvázolja, hogy miként lehetne egy absztrakt réteg-

modell-megközelítéssel szabványosítani a forenzikus tevékenységeket. Példaként ismerteti egy HTML fájl rétegbeli értelmezését a 10. ábra szerint.



10. ábra – Egy HTML fájl absztrakciós szintjei és rétegei (Forrás: [62 p. 6])

Véleményem szerint Brian Carrier modellje megfelelő kiegészítésekkel, illetve egyes elemzési funkciók egy rétegbe történő összevonásával alkalmassá tehető az információtechnológiai eszközök és rendszerek krimináltechnikai vizsgálatának általános leírására, illetve alapjául szolgálhat az egyes rétegekkel kapcsolatos kriminalisztikai funkciók meghatározására, továbbá az e funkciók megvalósításához szükséges szakértelem és az egyes szakterületek közötti interdependencia azonosítására. [64]

A szakértői vizsgálatok másik problémája, hogy a hazai szabályozásban jelenleg meglévő információtechnológiai kompetenciák nem illeszkednek az elvégzendő tevékenységekhez. A 9/2006. (II. 27.) IM rendelet – az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről – alapján a következő informatikai szakterületek vannak Magyarországon:

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver),
- informatikai biztonság,
- informatikai rendszerek tervezése, szervezése,
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység,
- számítástechnikai adatbázis, adatstruktúrák,
- szoftverek.

[65]

Ehhez a fenti informatikai szakterület felsoroláshoz nem áll rendelkezésre kompetencia leírás, csak a szükséges végzettséget írja elő a jogszabály.

A hazai szabályozással szemben az amerikai laboratóriumokban a számítástechnikai krimináltechnikai feladatokat a következőképp határozták meg:

- tartalomvizsgálat – annak megállapítása, hogy milyen típusú adatfájlok vannak a számítógépen,
- összehasonlítás – adatfájlok ismert dokumentumokkal és adatfájlokkal történő összehasonlítása,
- tranzakció/esemény időrendi megállapítása – annak megállapítása, hogy a vizsgált adatfájlok mikor és milyen sorrendben keletkeztek,
- adatfájlmentés – adatfájlok kimentése egy számítógépről vagy információtechnológiai rendszerből,
- törölt adatfájl helyreállítás – törölt adatfájlok helyreállítása egy számítógépen vagy információtechnológiai rendszerben,
- formátum átalakítás – adatfájlok átkonvertálása más, többnyire a további vizsgálatot végző számára használható vagy értelmezhető formátumra,
- kulcsszavas keresés – adatfájlokban szavak vagy kifejezések keresése, kilistázva a keresett szó vagy kifejezés valamennyi előfordulását,
- jelszó helyre állítás – titkosított fájlok megfejtéséhez szolgáló jelszavak helyreállítása,
- forráskód-elemzés – programok elemzése vagy forráskódok összehasonlítása.

[66]

Véleményem szerint az utóbbi felsorolás nem csak pragmatikusabb, hanem az informatikusok és az informatikában kevésbé járatos hatósági munkatársak számára is támpontokat nyújt a szakértőktől elvárható feladatokkal és az így kinyert bizonyíték természetével kapcsolatban. Értekezésemben erre a problémára is megoldást kívánok adni úgy, hogy az egyes forenzikus elemzési rétegekben végrehajtott funkciókhoz, vizsgálatokhoz hozzárendelem az végrehajtáshoz szükséges szakértelmet is – ezzel is kibővítve Brian Carrier alapmodelljét. Javaslatot teszek az egyes absztrakt vizsgálati rétegekhez kapcsolódó igazságügyi szakértői tevékenységekre, illetve kiegészítsem a jelenlegi szakértői kompetencialistát újabb tevékenységekkel, hogy az megfeleljen a szakmai kívánalmaknak, valamint a hazai informatikai igazságügyi szakértéssel kapcsolatos sajátosságoknak. [67]

II.1 Fizikai réteg

II.1.1 A fizikai réteg meghatározása

Brian Carrier vizsgálati rétegmodelljében a fizikai réteg (Physical Storage Media) a szabványos csatolókon keresztül elérhető fizikai tárolókat (merevlemez, memória chip és CD-ROM) és azok elemzését jelentette; ebben a rétegben a visszaadott adatalap-egység a bit. Ezen a szinten, de ettől elkülönült feladatként tekint a hálózatok és a memória vizsgálatára. A hálózatok esetén véleménye szerint a vizsgálandó alapegység a „csomag", illetve a hálózati naplók. A memória elemzés alapegysége Brian Carrier értelmezésében az értelmezett „kód" és „adat". [62 pp. 7–8]

Az én álláspontom ezzel szemben az, hogy a fizikai réteg fogalma kiterjeszthető valamennyi olyan fizikai entitásra, amelyen adatkezelési művelet történik – így különösen: adattárolás, adatfeldolgozás, adattovábbítás –, függetlenül az adatkezelés fizikai megvalósításától, az alkalmazott technológiai megoldástól.

Mivel azonban az értekezésem informatikai krimináltechnikai szempontú, ezért a továbbiakban csak az információtechnológiákkal kapcsolatos elemzésekkel foglalkozom.

Megállapításom szerint a fizikai rétegbeli vizsgálatok tárgya és alapegysége a bit – mind az adathordozó (fizikai tárolók), mind az adatfeldolgozó (processzor, memória), mind pedig az adattovábbító (hálózati közeg) esetében.

II.1.2 A fizikai rétegben elvégzendő általános feladatok, tevékenységek

A fizikai réteggel kapcsolatos tevékenységek célja az adathordozókon és a memóriában található, a számítógép-hálózaton áthaladó, illetve a processzor(ok) által épp feldolgozott valamennyi, az ügy szempontjából releváns jel detektálása, azonosítása, rögzítése, a rögzített adatok időpecséttel, ellenőrző kóddal (hash), esetleg digitális aláírással való hitelesítése. Az ebben a rétegben végzett adatmentés a későbbi vizsgálati lépések szempontjából alapvető fontosságú. A hiányos bitminta gátja lehet az adatok rekonstruálásának, mivel a számítógép-hálózaton továbbított jelek, a memóriában tárolt és a processzorok által a vizsgálatkor feldolgozott adatok irreverzibilis bizonyítékforrások. A hitelesítetlen adatforrás pedig a későbbiekben – a tárolás vagy további szakértői vizsgálatok során szándékosan vagy véletlenül – módosítható, ezért szakmai alapon kétségbe vonható a valódisá-

ga, vagyis bizonyítékként való felhasználhatósága jelentősen csökkenhet, esetleg arra alkalmatlanná válhat.

A kódolás-dekódolás során felmerül a tényleges csatornakódolás és a nyomrögzítéskor használt lehetséges kódolásnak a kérdése. Egy hibás dekódoló alkalmazásával rögzített adatfolyam alkalmatlan lesz bizonyítékként való felhasználásra.

A számítógép-hálózat fizikai rétegének elemzéséhez, az ezen áthaladó bitfolyam rögzítéséhez, a feldolgozással egyidejű adatrögzítéshez speciális szaktudásra van szükség az elméleti fizika, a gyakorlati villamosmérnöki ismeretek, az információ- és kódelmélet terén.

Az elkövetéssel egy időben végzett adatrögzítés a jelenleg hatályos Be. 200.§ (1)/c szerint titkos adatgyűjtésnek minősül, ami csak a 201.§-ban felsorolt speciális esetekben végezhető, és a 203.§ alapján bírói engedélyhez kötött az alkalmazhatósága. Az ilyen adatgyűjtést elsősorban a külön törvényben meghatározott szervek (Be. 204. §), a szakszolgálatok végzik, ha szükséges, bevonva az adattovábbítást végző szervezet képviselőit. A jelenleg hatályos Be. nem rendelkezik a különleges szakértelemmel rendelkező személyek[82] szükséges szerepéről a titkos adatszerzés során. [44]

Mivel a szakszolgálatok és a nyomozóhatóságok alapvetően nem információtechnológiai, telekommunikációs, számítógép-hálózati szakértők, és nem kötelező – csak a Be. 182.§ alapján lehetséges – különleges szakértelemmel bíró személyek bevonása a nyomrögzítési tevékenységbe, ezért felmerül a fizikai réteg vizsgálatával kapcsolatos szakmai kompetencia kérdése. Felmerül továbbá az, hogy a szükséges kompetencia milyen technológiával biztosítható, mivel szakértő bevonásának hiányában a nyomozóhatóság (vagy a szakszolgálatok) feladata a nyomrögzítés szakmai szabályainak megkövetelése, az elvárható gondosság szintjének biztosítása. Ez egy igen sajátos probléma, mert egy (információtechnológiai, számítógép-hálózati) szakmai szempontból laikus szervezetnek kell egy általa csak részben vagy egyáltalán nem ismert terület szabályinak betartásáról, betartatásáról gondoskodnia.

Az én álláspontom az, hogy ilyen esetekben a titkos adatgyűjtést végző szervezetnek igazságügyi szakértőt kellene kirendelnie szaktanácsadóként a nyomrögzítés elvégzésére, vagy a nyomrögzítés szakmai feltételeinek felügyeletére. Ez a nehézség részben kezelhető, tekintettel arra, hogy a hálózati adatforgalom rögzítése elterjedt hálózati technológiák

[82] Például nem szakszolgálati állományú szakértők, szaktanácsadók.

esetén arra alkalmas hardver és szoftver segítségével automatizálható. Sokat segítene ebben a kérdésben (is), ha ilyen típusú vizsgálatokkal, nyomrögzítéssel kapcsolatos igazságügyi szakértői kamarai módszertani levelek megszületnének, és egységesen kiadásra kerülnének a nyomozóhatóságok, a szakszolgálatok és az igazságügyi szakértői kamara tagjai számára. [64]

II.1.3 A fizikai rétegben alkalmazott jellemző hardver és szoftver eszközök

III.1.3.1 Adatforgalom mentése

Az igazságügyi szakértés során olyan eszközöket kell alkalmazni, amelyek nem befolyásolják a vizsgált rendszerek működését, vagy ha mégis, akkor ismert az alkalmazott eszköznek a mért folyamatra gyakorolt hatása.

Elérhetők olyan ethernet és optikai vizsgálati eszközök (network tap), amelyek késleltetés nélkül és a hálózati forgalomba való legkisebb beavatkozás nélkül képesek a vizsgáló számítógép felé duplikálni az adatforgalmat. A hubokkal, vagy aktív hálózati eszközökkel ellentétben ezek az eszközök tiltanak minden, az elemzési vizsgálati portokról eredő adatforgalmat, így a mérőeszköz esetleges hibája miatt „elszabadult” bitek nem szennyezik az elemzendő adatforgalmat. Ilyen eszközre mutat példát a 11. ábra.

Teeny Tap 10/100 Copper Ethernet hálózatokhoz

GigaBit Fiber Teeny Tap optikai hálózatokhoz

11. ábra – NetOptics hálózati írásvédők (forrás: www.netoptics.com)

Speciális célhardver hiányában lehetséges hagyományos hálózati eszközök használata (router, switch), csakhogy ezek használatakor módosítani kell az eszközök konfigurációját, hogy a mikro szegmentációt, illetve a forgalomirányítást (routing) kiiktassuk/módo-

sítsuk, és a forgalom elemzéséhez és rögzítéséhez használt eszközre irányítsuk a forgalmat.

A hardver mellett szükséges valamilyen elemző-adatrögzítő szoftvert is alkalmazni, amelyhez biztosítani kell, hogy az operációs rendszer képes legyen a hálózati kártyára érkező valamennyi jelet fogni (promiscuous mode). Ehhez Windows esetében a hálózati protokoll-kezelést és a hálózati kártya hozzáféréseket módosító a winpcap[83] vagy az airpcap[84] szoftverekre és a Wireshark[85] protokollelemző szoftverre van szükség. [68]

A vezeték nélküli hálózatok esetén szükség lehet a hálózati forgalom mellett a hálózatok adás-vételi karakterisztikájának a megállapítására – a hálózatok felderítésére – is.
A vezeték nélküli hálózatok felderítéséhez szükséges

- hardver eszközök:
  - hordozható számítógép,
  - WiFi antenna és kártya,
  - GPS;
- szoftver eszközök:
  - számítógép-hálózatfigyelő szoftver,
  - térinformatikai alkalmazás.

A számítógép-hálózatok technikai felderítése során szerzett adathalmaz azonban önmagában nem vagy csak nehezen, vagy nem teljes körűen értelmezhető a laikusok – nem informatikai szakértők, így a nyomozásban, a vádemelésben, vagy az ügy megítélésben résztvevő hatóságok tagjai – számára. A vezeték nélküli hálózatok vizsgálatának kulcsfontosságú eleme egy GIS (Geographic Information System) vagy térinformatikai alkalmazás, amely lehetővé teszi az összegyűjtött információknak feldolgozását és térbeli megjelenítését.

[83] L. www.winpcap.org

[84] L. www.cacetech.com/products/airpcap.html

[85] L. www.wireshark.org

Egy általános célú térinformatikai alkalmazás a mért adatok helye és a helyhez kapcsolódó geográfiai, topográfiai, közmű és egyéb adatok alapján képes térbeli elemzést készíteni az alábbi témákban:

- **hely**, azaz vizsgálható, hogy mi található egy adott helyen,
- **körülmény**, azaz vizsgálható, hogy hol van a keresett objektum, tereptárgy vagy eszköz,
- **trendek**, azaz vizsgálható, hogy mi változott meg, illetve a változások milyen jellegzetességet mutatnak,
- **útvonal**, azaz vizsgálható, hogy melyik a legkedvezőbb út egy pontból egy másikba,
- **jelenség**, azaz vizsgálható, hogy mi a jelenség, illetve mik a jelenséget meghatározó legfontosabb tényezők,
- **modellezés**, azaz vizsgálható, hogy mi történik, ha a környezet valamely paramétere megváltozik,
- a feltett kérdésekre és az elemzések adataira vonatkozó – **vizuális megjelenítésre vonatkozóan** – jelek, grafikus ábrák, képek stb. [69 p. 25]

Az így kapott vizuális elemzések már alkalmasak a szakértői megállapítások demonstrálására az informatikában nem járatosak számára is. Egy professzionális GIS szoftverrel kiegészített WiFi hálózat vizsgálata az elemzési lehetőségek széles tárházát biztosíthatja, például figyelembe veheti az épületek szerkezeti elemeinek vagy a tereptárgyaknak a rádiófrekvenciás jelekre gyakorolt csillapító, reflektáló hatását.

Az elemzőrendszer másik kritikus pontja a vezeték nélküli hálózati (WiFi) kártya, mivel ennek a rádióvezérlő chipje meghajtó programjának (driver) támogatnia kell a hálózat monitorozását (raw monitoring mode) és a 802.11b, a 802.11a, a 802.11g és a 802.11n hálózati forgalom lehallgatását. [68]

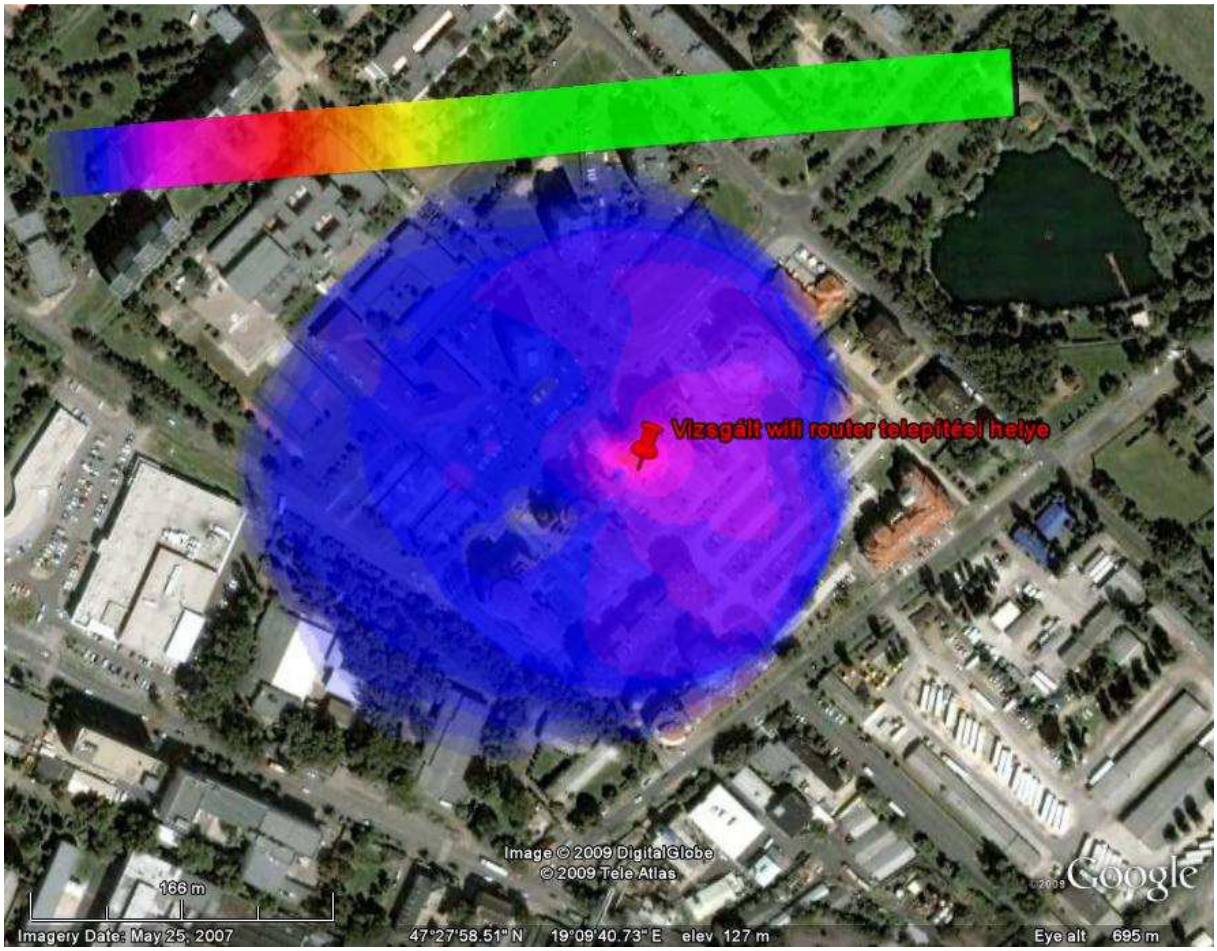
A többi hardver elemmel szemben a gyakorlatban nem merülnek fel problémák, minden hordozható számítógép és az ehhez csatlakoztatható GPS modul megfelel a vezeték nélküli hálózatok felderítéséhez.

A vezeték nélküli hálózatok felderítésének lépései a következők:

1) adatgyűjtés,
2) a hálózat térerejének karakterisztikáját jelző „hőtérkép” elkészítése,
3) a gyűjtött adatok térképen való megjelenítése,
4) elemzés.

[57] [69]

A vezeték nélküli hálózat felderítés vizualizált eredményei felhasználhatók például egy WiFi hálózat jelerősségének feltérképezésére, a lehetséges kapcsolódási pontok meghatározására. A jelerősség térképre helyezett ábrázolása segítségével könnyen meghatározható például, hogy valaki hozzáférhetett-e valahonnan egy nyílt WiFi végponthoz, ezzel megerősítve vagy cáfolva egy feltételezett elkövetési magatartást. Ilyen jelerősség vizualizációra mutat példát a 12. ábra.



12. ábra – A vizsgált számítógép-hálózat lefedettsége Footprint segítségével a Google Earthben ábrázolva (forrás: Illési Zsolt)

Cellás rendszerek, mobiltelefonok[86] adatforgalmának mentése – kivéve, ha azt törvényi felhatalmazás és engedélyezés mellett arra feljogosított szerv, például szakszolgálat végzi – jogsértő, így ezzel az értekezésemben nem foglalkozom[87].

III.1.3.2 Adattároló mentése

Egy informatikai igazságügyi szakértő életében a leggyakrabban előforduló nyombiztosítási mód az adathordozók adattartalmának az eredetivel bitről-bitre egyező mentése. A feladat végzésekor a terhelt adathordozóját[88] úgy kell lementeni, hogy a másolat adattartalma az eredetinek pontos és hiteles másolata legyen. Erre alapvetően két megoldás létezik: az írásvédők és valamilyen másoló program, vagy lemezmásoló hardver alkalmazása.

Az adattárolók mentésének az egyik – másolási módszertől független – gyakorlati problémája a számítógép perifériák típusainak[89], csatlakozóinak[90] jelentős száma. A mentés megkezdése előtt alaposan fel kell mérni, hogy milyen eszközökkel és azoknak milyen interfészeivel, csatolóival fog megküzdeni a szakember, de így is érhetnek meglepetések.[91] A 13. ábra illusztrálja a jelenlegi memóriakártyák sokszínűségét. A sikeres mentésnek tehát feltétele egy komoly fizikai interfész és adapter-készlet használata.

---

[86] GSM, HSDPA, TETRA stb.

[87] Mindamellett az ehhez szükséges hardver és szoftver technológia már mindenki számára elérhető; l. http://www.grc.com/sn/sn-213.pdf

[88] Számítógépének merevlemezét, USB-kulcsát stb.

[89] SATA 1.0/ 2.0/ 3.0 stb.

[90] eSATASp, eSATA I/ L stb. port.

[91] Egy ügyfél felkért több szerver SCSI csatolású RAID-be kötött merevlemezének a lementésére. Az eszközök típusa és kapacitása – többek között – a mentés megkezdése előtt többször is egyeztetve lett a rendszergazdával, azonban csak helyszínen derült ki, hogy az „SCSI" a „SAS" (Serial Attached SCSI), aminek a csatolófelülete és az adatátviteli protokollja jelentősen eltér az SCSI-től. A helyszínen derült ki az is, hogy Magyarországra a vizsgálat idején még nem hozott be SAS írásvédelmi eszközt a legnagyobb hazai forenzikus beszállító.

13. ábra – Memóriakártyák
(forrás: www.trustedreviews.com)

A szervermentés egyik kulcskérdése az esetleges RAID vezérlők, azok típusának és beállításainak azonosítása, mivel az elemzés során a vizsgálatot végzőnek rekonstruálnia kell a RAID tömböt, ami esetenként hosszantartó, kínos „try-and-error" jellegű próbálkozásokkal hozhat csak eredményt.

Az adattárolók mentése közben, amennyiben a másolás közben valamely bit hibás, azaz a szokásos módszerekkel nem lehet kiolvasni, akkor a konvenció szerint a cél adathordozón a hibás értékeket `hx0`[92]-val kell feltölteni. Így biztosítható, hogy a későbbi keresések során „steril" adatokat talál az elemző, és nem valamilyen véletlen adattartalmat, amit akár a véletlen folytán terhelő adatként is értelmezhetne. A hibáknak `hx0`-val való prezentálása lehetővé teszi azt is, hogy az adathordozó adattartalmának hitelesítésre számított hash érték azonos legyen két egymást követő ellenőrzéskor[93].

Az adatmásolás lehet

- diszk-diszk vagy
- diszk-fájl típusú.

Diszk-diszk mentésnél az eredetivel azonos méretű médiára történik a másolás. Amennyiben a cél adathordozó nagyobb, mint a forrás, úgy a fennmaradó területet vagy `hx0` értékekkel kell felülírni, vagy a lemezgeometriát kell módosítani az ún. Device Configura-

[92] Hexadecimális „`0`" értékkel.

[93] Amennyiben az adathordozó állapota nem romlott, a hibák száma nem nőtt a két vizsgálat között eltelt időben.

tion Overlay vagy DCO értékek módosításával, hogy az megfeleljen az eredeti lemezének. Ez a módszer megfelel a lemezek „klónozásának”, és akár használatba is lehet venni a másolatot. Azután a forrás merevlemezt tartalmazó számítógépbe visszahelyezve az operációs rendszer elindulhat, és rendelkezésre állhat az eredetivel azonos működőképes rendszer.

Diszk-fájl mentésnél a forráslemez tartalmát a céllemez fájlrendszerében fájlokba másoljuk. A fájlok mérete tetszőlegesen változtatható[94]. Fájlba mentésnél a másolatról – bár megegyezik az eredetivel – nem lehet erről elindítani a forrásrendszert. A leggyakoribb formátumok a „`dd`”[95] és az „`E01`” (Encase) formátum. Az `E01` formátum előnye, hogy tömörített formában tárol, illetve hogy fájlonként külön-külön is fejlécet tartalmaz, és valamennyi darabhoz külön-külön is számít ellenőrző hash értéket.

Itt kell megjegyezni azt a sajnálatos hazai gyakorlatot, hogy a büntetőeljárások során rendszeresen elmarad az adathordozóknak, mint bűnjelforrásoknak a rögzítése; a vizsgálatokat a lefoglalást követően sokszor kell az eredeti adathordozón elvégezni. A másolás elmaradása miatt a gyakorlatban sokszor sérül az adatok hitelessége, nem igazolható, hogy a lefoglalt adathordozón csak az az adat – és nem több, nem kevesebb – volt, mint ami az elemzést megelőzően. [70] [71]

Forenzikus írásvédők

Az írásvédők olyan hardver vagy szoftver megoldások, amelyek az adathordozó felé irányuló valamennyi írással/adatmódosítással járó műveletet szűrnek, és csak a lekérdezéseket engedik tovább.

[94] Ez a méret az egyes hardver és szoftverek alapbeállításai alapján 1,5-2GB.

[95] A *nix operációs rendszerek disk dupe parancs kimeneti fájlformátuma.

A szoftveres megoldások közül a legolcsóbb a kötetek írásvédett felcsatolása. *nix rendszereknél ezt a

```
# mount -r -t ufs -o ufstype=[fájlrendszer] /[forrás meghajtó] /[csatolási pont]
```

parancs használatával lehet megoldani.

Windows rendszereknél az USB-s eszközök írásvédelmét például a Thumbscrew[96] program használatával, vagy a `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect` registry kulcs módosításával lehet elérni. A fenti szoftveres megoldások az ár-érték versenyt megnyerik, de ennek az ára írásvédelem minőségnek bizonytalansága[97], de hardveres megoldás hiányában – például hardveres RAID tömbök adatainak lementésére – „B" tervként megfelelnek a célnak.

A hardveres megoldások (l. 14. ábra) előnye a nagyobb adatátviteli sebesség és a garantált írásvédelem[98]. A hardveres megoldások előnye, hogy nagy általánosságban valamilyen „csomagban" szállítják őket, ami többféle eszközhöz való csatolókat, átalakítókat, táp- és adatkábeleket tartalmaz, jelentősen leegyszerűsítve a munkavégzést.

Tableau
T6es SAS írásvédő
(forrás: www.tableau.com)

WiebeTech
Forensic UltraDock IDE/SATA írásvédő
(forrás: www.wiebetech.com)

14. ábra – Hardver forenzikus írásvédők

[96] L. http://www.irongeek.com/i.php?page=security/thumbscrew-software-usb-write-blocker

[97] Az operációs rendszertől függ, hogy megfelelően védje az adathordozót valamennyi írási kísérlettől – így a kernel szintűektől is).

[98] A hardver nem engedi át az ismeretlen parancsokat, az ismertek működését pedig laboratóriumokban vizsgálják.

Az írásvédők alkalmazásával lehetőség nyílik az adattárolón lévő adatok vizsgálatára úgy, hogy nem kell az egészről másolatot készíteni, illetve valamilyen másoló program[99] használatával – természetesen egy számítógép közbeiktatásával – bitszintű másolat készíthető. [70] [71]

Speciális írásvédők

A forenzikus írásvédők egyik különleges fajtája nem a lemezek megtekintését vagy a másolást segíti, hanem lehetővé teszi, hogy a vizsgálatot az eredeti számítógépen lehessen elvégezni úgy, hogy a bekapcsolás és használat során bekövetkező módosítások mégsem érintik az eredeti lemez tartalmát (l. 15. ábra).

Ezt úgy tudják elérni, hogy az írásvédő a forráslemez felé nem engedi át az adatmódosítással járó parancsokat, hanem az írni/módosítani kívánat adatokat megduplázza egy átmeneti tárolóként szolgáló beépített merevlemezen, és az írási műveleteket ezen a másolaton hajtja végre. Az árnyékmeghajtó működése transzparens a merevlemezt felhasználó számítógép számára, nem érzékeli a közbeékelt eszközt sem, valamennyi műveletet végre tudja hajtani.

Ez a megoldás kiválóan alkalmas például tárgyalótermi demonstrációk során, vagy szembesítéskor; be lehet mutatni a rendszerfunkciókat, a működést, illetve a tárolt adatokat, közvetlenül a vizsgált számítógép felhasználásával.

Hátránya a viszonylag magas ár és az, hogy csak korlátozott eszközökhöz (IDE, SATA) érhető el ilyen eszköz. Egyszerűen helyettesíthető az eredeti lemezről készített klón lemezzel, de ezek elkészítése időigényes. [70] [71]

[99] A *nix operációs rendszerek `dd` parancsa, vagy az AccessData ingyenesen is hozzáférhető FTK Imager programjának Ez utóbbi letölthető a következő címről: http://accessdata.com/downloads/current_releases/imager/AccessData%20FTK%20Imager.exe

15. ábra – Voom Shadow 2
Forensics merevlemez írásvédő – lemezhasználat közbeni írásvédelem
(forrás: www.voomtech.com)

Forenzikus másolók

A forenzikus másolók olyan eszközök, amelyek külön számítógép közreműködése nélkül képesek különféle[100] merevlemezekről másolatot készíteni, a másolatok hash értékeinek kiszámítására, ellenőrzésére és a tevékenységek naplózására.

A 16. ábrán is látható hardveres megoldások előnye a nagy másolási sebesség, az általános számítógépekhez képest a környezeti körülményekkel szembeni nagyobb ellenállóság és az egyszerű kezelhetőség, viszont hátrányuk a szoftveres („0Ft”-os) megoldásokhoz képest magas árúk.

A piacon rendelkezésre álló modellek között vannak 1:1 másolat és 1:n másolat készítésére szolgálók is. Az utóbbi eszközöket többnyire elosztott vizsgálatokat végző intézmények, bizonyítéktárakat is kezelő szervezetek alkalmazzák[101].

[100] Ezek többnyire IDE/ ATA/ PATA és (e)SATA csatalójú lemezek.

[101] Például egy lemezt a bűnjeltár vagy az archívum számára készítenek el, 1-1 lemezt elküldenek két egymástól független vizsgálónak, hogy így is növeljék a vizsgálat(ok) hitelességét és megbízhatóságát.

Tableau
TD1
(forrás: www.tableau.com)

Voom
SuperDuper
(forrás: www.voomtech.com)

16. ábra – Forensics merevlemez másolók

A hardveres forenzikus másolók esetenként alkalmasak a merevlemezek formázására vagy „sterilizálására”[102], és így biztosítható a céllemezek újrahasznosítása anélkül, hogy korábbi ügyek adatai összekeverednének az új ügy adataival.

Itt lehet megemlíteni azokat a céleszközöket, amelyek úgy írják felül az adattárolón található adatokat, hogy azt a későbbiek során semmilyen eszközzel nem lehet helyreállítani. A felülírás ilyen esetben több menetben és változó bitmintával történik. [70] [71]

III.1.3.3 Memória mentése

A memória mentésére csak működő számítógépek esetén van lehetőség. Speciális körülmények között megoldható a kikapcsolt számítógépek memóriájának lementése[103], azonban ez utóbbi technika a forenzikus vizsgálatok gyakorlatában nem jellemzően használt, így ezzel a továbbiakban nem foglalkozom.

A működő számítógép memóriájának mentésére akkor van szükség, ha a vizsgált

- számítógéphez titkosított fájlrendszerek vannak csatolva,
- számítógép titkosított csatornán keresztül kommunikál – a memória tartalmazza a hozzáféréshez szükséges kulcso(ka)t,

[102] Valamennyi adatot azonos bitmintával, jellemzően `hx0` értékkel, felülírni.

[103] L. wikimedia.org/wikipedia/en/wiki/Cold_boot_attack

- számítógéppel kapcsolatban lényeges, hogy a felhasználó milyen tevékenységeket folytat a nyomrögzítéskor – hiszen a memória tartalmazza azokat az adatokat is, amelyeket a rendszer nem ír ki a merevlemezre –, például sandboxban/homokvemben futó chat alkalmazások vizsgálatakor,
- számítógépet megfertőző kártékony kód működését kell elemezni – a memória tartalmazhat a hálózati megnyitott kapcsolatokra, az alkalmazott titkosításra, a parancsszerverekre vonatkozó adatokat.

A memória megfelelő szoftveres mentéséhez többnyire rendszergazdai jogosultságokra van szükség, ennek hiányában vagy csak a rendszer hibázásra bírásával és a hiba eredményeként például a rendszermemória „kidumpolásával" lehet eredményhez jutni, vagy csak részeredményeket lehet produkálni.

A rendszermemória hibázását csak célzottan, a rendszer és rendszer szoftverkomponensek pontos ismeretében lehet elvégezni. Ez a technika szintén nem javasolt, mivel a hibák esetenként kiszámíthatatlan eredményre vezetnek, és előre nem lehet minden esetben felkészülni a hatásukra.

Több gyártó is kínál főleg USB kulcsokra előretelepített segédprogramokat, amelyek lehetővé teszik a memória mentését[104]. A Microsoft is előrukkolt egy COFEE[105] szoftvergyűjteménnyel, amely az élő rendszerek vizsgálatát teszi lehetővé[106]. [72]

A szoftveres megoldásokra a hekkerek is felfigyeltek, és elkészítették az MS COFEE ellenszerét a DECAF[107]-t, ami érzékeli a COFEE-t tartalmazó USB kulcsot és a beállításoknak megfelelően kikapcsol és/vagy törli a naplófájlokat, és/vagy üzenetet küld a felhasználónak.[108]

---

[104] Ilyen eszköz például az e-Fense LiveResponse, l. http://www.e-fense.com/live-response.php

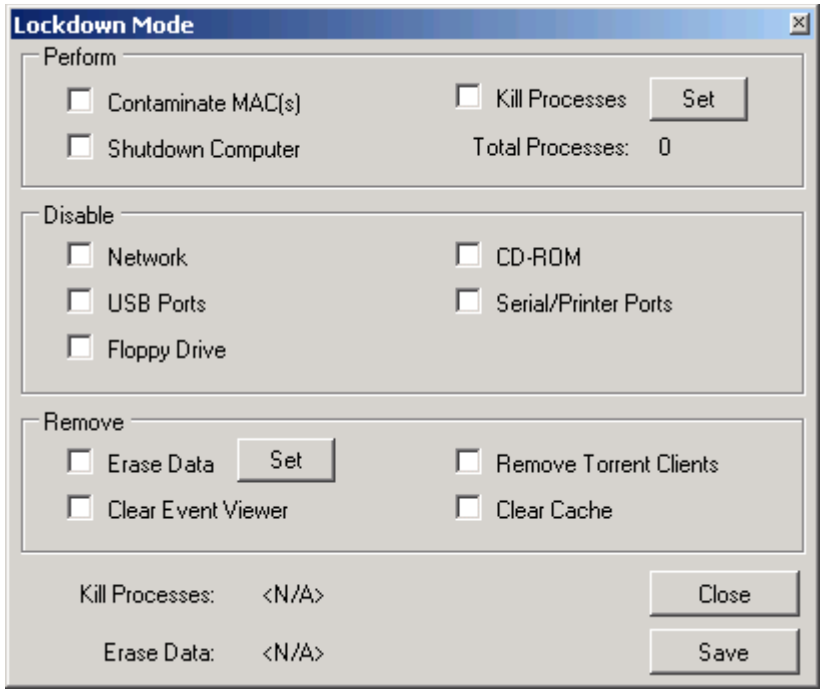
[105] Computer Online Forensic Evidence Extractor.

[106] L. https://www.microsoft.com/industry/government/solutions/cofee/default.aspx

[107] Detect and Eliminate Computer Assisted Forensics.

[108] A DECAF-t ugyan már nem lehet elérni az interneten – még a weblapot is törölte a program írója –, de az eszköz ismeretében biztos lehet benne mindenki, hogy ilyen és ehhez hasonló programok várakozhatnak az élő rendszerekben csak egy forenzikus eszközre várva, hogy aktiválódjanak.
(Ez egyébként jól példázza azt a macska-egér játékot, ami a bűnelkövetők és az igazságszolgáltatás között a kibertében is zajlik, illetve arra is rávilágít, hogy az élő rendszerek vizsgálata mennyi problémát rejt.)

A 17. ábra a DECAF konfigurációs menüjét mutatja, megmutatva, hogy milyen sokrétű önvédelmi beállításokra képes egy ilyen antiforensic segédprogram, amennyiben érzékeli egy COFEE behelyezését:



17. ábra – DECAF konfigurációs felületének részlete (forrás: Illési Zsolt)

Esetenként lehetőség van a fizikai memória közvetlen elérésére, például FireWire kapcsolaton keresztül, a DMA memória kontroller közvetlen elérésével, sajnos – legalább is forenzikus értelemben sajnos – nem minden vizsgált eszköz rendelkezik csatlakozó felülettel. [71] [73] [74]

III.1.3.4 Mobiltelefon és PDA adatmentő eszközök

A mobiltelefonok, a kézi számítógépek, a digitális személyi asszisztensek[109] ugyanolyan jó, sőt esetenként hasznosabb bizonyítékforrások lehetnek, mint az asztali számítógépek és a laptopok, hiszen ezeket az eszközöket a felhasználóik személyes tárgyként kezelik, folyamatosan maguknál tartják, SMS és e-mail üzeneteket váltanak rajtuk keresztül, nyilvántartják a teendőiket a naptárbejegyzéseiket.

A mobil eszközökre az egyre nagyobb „intelligencia” a jellemző. A jelenlegi okostelefonok processzorteljesítménye, memória és tároló kapacitása, funkcionalitásának gazdag-

[109] Personal Digital Assistant vagy PDA – a továbbiakban együttesen: mobil eszközök.

sága megfelel, sőt ma már meghaladhatja az egy évtizeddel ezelőtti asztali csúcsgépek teljesítményét. A telefonok már nem csak telefonálásra, hanem komplex információtechnológiai szolgáltatások nyújtására is képesek, akár internet kiszolgáló alkalmazásokat, web/ftp szervereket is futtathatunk rajtuk; vagyis úgy kell kezelni őket, mint a „nagytestvéreiket" a „rendes" számítógépeket[110].

A mobil eszközöknél az adattárolóknál a csatlakozókkal kapcsolatban már leírt problémák halmozottan jelennek meg, itt jelenleg az alkalmazott csatolók 80%-ot nem 2-3, hanem jóval több lehetséges változatból kell kiválasztani[111].

Az alábbi ábra a leggyakoribb mobiltelefonok adatkábel-végződéseit mutatja be:

18. ábra – Mobiltelefonok adatkábel-végződései
(forás: http://mobiledit.com/forensic/fcase.asp)

A mobiltelefonok vizsgálatakor az általános követelmények mellett gondoskodni kell a telefonok leárnyékolásáról, arról, hogy a telefon ne kapcsolódhasson rá a szolgáltató hálózatára, hogy az utolsó hozzáférés adatai ne módosuljanak, illetve hogy a vizsgálatokat

[110] A mobil eszközök (funkcionalitásban ekvivalensek lehetnek, csak teljesítményben maradnak el a „kistestvérben" alkalmazott processzor, memória stb. fizikai korlátai miatt.

[111] Jó példa erre a Nokia telefonoknál tapasztalható „szabványosítás", vagyis az egyedi csatolók – például DKU-5 adatkábel – mellett a telefonok több különböző USB (CA-101/ mikro-USB, DKE2/ mini-USB adatkábelek) csatolóval is fel vannak szerelve.

ne zavarja meg egy hívás/üzenet, illetve hogy a használó vagy egy bűntársa távolról ne tudja törölni vagy módosítani az eszközökön tárolt adatokat. [70] [71] [75] Egy ilyen eszközt mutat be a következő ábra:

19. ábra – Paraben Wireless StrongHold Box
(forrás: http://www.paraben.com/stronghold-box.html)

II.1.4 A fizikai réteg által megkívánt szakmai kompetencia

Mivel a fizikai réteghez köthető tevékenységek során a fizikai közegben rögzített biteket kell helyreállítani és rögzíteni, ezért ehhez a feladathoz fizikus vagy villamosmérnöki ismeretekre van szükség. A fizikai réteggel kapcsolatos tevékenységek során az információtechnológiai rendszer hardver komponenseiből kell adatokat menteni, illetve a hálózatok átviteli közegében kódolt adat dekódolására speciális eszközök használata szükséges, amihez az átvitel- és kapcsolástechnikai rendszerek mélyreható ismerete szükséges.

A feladat elvégzése informatikai szakemberekre is rábízható, tekintettel arra, hogy az informatikusi képzésnek is része a hardver, az adathordozók és számítógép-hálózatok – főleg felhasználói, rendszergazdai szintű – ismerete. Az informatikai szakképzésben a kódolás finom részleteit a hardver architektúra, az abba integrált firmware[112], illetve az információtechnológiai rendszerek és komponensek operációs rendszerei általában elrejtik az általános informatikusok elől, a sérült fizikai kódolás, a hardver komponensek meghibásodása túlmutat az ő kompetenciájukon[113]. Ezért úgy gondolom, hogy a hardverhibák és a sérült fizikai kódolás javítása csak speciális – főleg villamosmérnöki – kompe-

[112] A firmware (ejtsd: förmver) olyan, közvetlenül egy hardverhez kapcsolódó, abba valamilyen adathordozó chipbe integrált programokat és/vagy adatstruktúrákat jelent, amely a hardver eszköz vezérlését, a magasabb szintű programok vagy közvetlenül a felhasználók kiszolgálását végzi.

[113] A kódolás és hardverelemek hibájának elemzése elsősorban tervező-fejlesztői és nem üzemeletetői feladat.

tenciával látható el. A szakértőnek ilyen esetekben mindenképp fel kell hívnia a kirendelő hatóság figyelmét a hibára, annak természetére és a kompetencia hiányára, vagy a hibajavításhoz szükséges speciális kompetencia meglétére.

A fizikai közegek adat-, illetve csatornakódolása nagymértékben szabványosított, és ezek a feladatok automatizálhatóak, véleményem szerint az adatrögzítési tevékenységek – megfelelő módszertani útmutatás mellett – alacsonyabb kompetenciaszintű munkatársakra is rábízhatók. A nyomozóhatóságok munkatársai, a munka jellegéből következően az általános bűnügyi technikusok, viszonylag gyorsan felkészíthetők lennének a fizikai réteghez köthető információtechnológiai feladatokra, így alkalmazásukkal a bűnügyi költségek jelentős része megtakarítható lenne. [70] [71]

II.2 Médiamenedzsment réteg

II.2.1 A médiamenedzsment réteg meghatározása

Brian Carrier vizsgálati rétegmodelljében a médiamenedzsment réteg (Media Management) a fizikai tárolók tárolási egységeinek – merevlemez partícióknak – a helyreállítását, azonosítását és elemzését jelenti, az elemzés által visszaadott érték valamilyen tárolási struktúra alapja. A médiamenedzsment réteg vizsgálata nem minden esetben értelmezhető, például amennyiben egy adatbázis-kezelő közvetlenül particionálás nélküli teljes merevlemezt használ. A fizikai tároló médiumelemzésből következő, a kötetelemzéssel azonos szinten lévő feladatként említi a memóriaelemzést is, amely feladat a bitek folyamat és rendszeradatként való értelmezését jelenti, ami magában foglalja a kód és az azt futtató folyamat megfeleltetését, valamint a máshol nem tárolt szenzitív információk kinyerését is. [62 pp. 7–8]

Megállapításom szerint a médiamenedzsment réteg fogalma alkalmazható valamennyi, a fizikai rétegben összegyűjtött bitláncra, mely valamilyen struktúra alapján egy adattárolási egységként értelmezhető, így a fogalom kiterjeszthető a hálózaton továbbított adatokra, ahol az elemzés során visszaadott érték a hálózati csomag, memória esetén a memóriatérkép, az adat, kód szegmensekkel, illetve a processzorok vagy a regiszterek elkülönített értékei, illetve az egyes gyorsító tárak tartalma.

II.2.2 A médiamenedzsment rétegben elvégzendő általános feladatok, tevékenységek

Az információtechnológiai-kriminálltechnikai vizsgálat második lépcsője során a cél a fizikai rétegben gyűjtött adatok elemzése, a hálózaton áthaladó bitfolyam, a memóriában vagy más adathordozón tárolt, illetve a processzor által feldolgozott adatok rögzítését követően az elsődleges adatkonténerek[114] azonosítása és elkülönítése egymástól.
Ide tartozik továbbá a vizsgált adathordozón a virtualizált alkalmazások, tárhelyek felkutatása és helyreállítása és adatainak feltárása[115]. [76]

A médiamenedzsment rétegben végzett számítógép-hálózati vizsgálatok során az egyik szakmai problémát az jelenti, hogy a bitfolyam elvileg többféleképpen értelmezhető, az egységes – valamennyi kódolási eljárásban egységesen alkalmazott – irreducibilis[116] kódok használata nem jellemző. Amennyiben a hálózati keretek például átviteli zavarok, hibák hatására sérültek, nem különíthetők el egyértelműen egymástól, így az alkalmazott hálózati csomagok, hálózati protokollok, protokoll hierarchiák mélyebb ismeretére, illetve mintaillesztő algoritmusok használatára is szükség lehet a legvalószínűbb keretfolyam előállításához.

Erre egy példa egy bitfolyam hexadecimális formában, ARP csomagként való 2 lehetséges értelmezése:

1. lehetséges ARP csomag kezdete

```
00 01 08 00 06 04 00 02 00 e0 00 10 80 00 60 4d 01 76 ff ff ff ff ff ff 9f 7d 03 55
```

2. lehetséges ARP csomag kezdete

20. ábra – ARP csomag lehetséges értelmezése egy bitfolyamban (szerk.: Illési Zsolt)

A számítógép-hálózati vizsgálatoknál a médiamenedzsment rétegben kell először a csatorna-dekódolás esetleges hibáit, zavarait is figyelembe venni, ebben is a protokollhie-

[114] Hálózati keretek, merevlemez/adattároló struktúrák.

[115] A vizsgálat során:
- hardver/platform,
- (logikai) desktop,
- szoftver (operációsrendszer, alkalmazás, szolgáltatás),
- tárhely,
- hálózat

virtualizáció nyomait kell/lehet keresni és az adatait helyreállítani.

[116] Egyértelmű dekódolást biztosító (prefix tulajdonságú) kódolás, ahol a kódszavak mind különböznek egymástól, továbbá egyik kódszót sem kaphatjuk meg a másikból kódjelek utáni írásával.

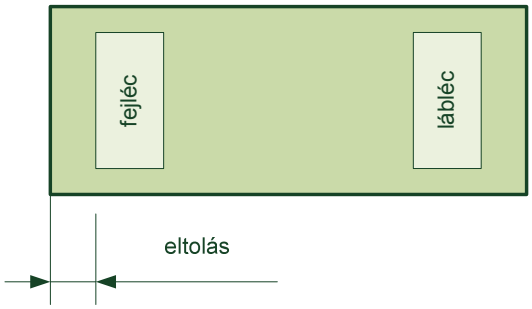
rarchia mélyebb ismerete, azaz, az alkalmazott hibafelismerő és hibajavító kódolás szükséges. [64]

Adathordozók analízisekor vizsgálni kell például a partíciók egymáshoz képesti helyzetét, hiszen ezek elhelyezkedhetnek közvetlenül egymás után, lehetnek kisebb-nagyobb nem-használtként regisztrált nem-szektorok a partíciók között, vagy épp ellenkezőleg, a partíciós tábla bejegyzései alapján átfedhetik egymást. Az esetleges anomáliáknak lehet oka szándékosság[117] vagy a partíciós tábla hibája. Ezen a szinten kell azonosítani a partíciók típusait, a fájlrendszereket, mivel ez biztosítja azt, hogy a következő lépés során helyesen értelmezett fájlokat lehessen elemezni.

Amennyiben felmerül a gyanú, hogy hiba vagy szándékosság miatt adatok lehetnek az egyébként nem használt területeken, úgy szóba jöhet az adat(vissza)vésés (data carving), ami arról szól, hogy a fájloknak többnyire van valamilyen, a fájltípusra jellemző

- fejléc formátuma, azaz egyedi fejléc bitminta,
- lábléc formátuma, azaz egyedi lábléc bitminta,
- egy eltolási (offset) értéke, ami a fájlkezdet és a fejléckezdete közötti bitek számát határozza meg[118].

Az adatvisszavésés elvét szemlélteti a következő ábra:



21. ábra – Az adat(vissza)vésés elvi ábrája (szerk.: Illési Zsolt)

[117] Például ha a terhelt előre készült arra, hogy összezavarja a vizsgálatot végzőt, vagy adatokat rögzített a látszólag nem particionált területekre, így rejtve el azt a laikusok és a kisebb felkészültségű vizsgálók elől.

[118] A fájl kezdete és a fejléc közötti „haszontalan” adatterületen mindenféle véletlen karakter lehet, ami általában a fájl hasznos információt tartalmazó részét nem érinti, csak valamilyen fix hosszúságú, véletlenszerű technikai adatokat tartalmaz.

Ez a megközelítés az adattárolókon a partíciós táblák, a fájlrendszer-leírók[119] sérülésekor, vagy egyszerű szteganográfia alkalmazásának gyanúja esetén is fájltöredékekből való helyreállításhoz használható.

A fejléc adatai, a lábléc adatai és az esetleges offset együttesen adják a fájlra jellemző mágikus számokat, amelyekre az alap fájlvésési technikák épülnek. Ilyen mágikus számokat lehet találni például a http://www.garykessler.net/library/file_sigs.html honlapon.

Az egyik legismertebb fájlminta a JPEG fájloké, amelynek jellemző értékei:

- fejléc: `0xFFD8,`
- lábléc: `0xFFD9,`
- offset: `0.`

Ezek alapján már egy egyszerű hexaeditorral is hatékonyan lehet adatokat találni a „bitdzsungelben".

A hibaarány csökkentése érdekében lehetséges ezeket a mágikus számokat továbbpontosítani, és például a `0x FF D8 FF E0 xx xx 4A 46 49 46 00` hexa (azaz a „`ÿØÿà..Exif.`" ASCII) fejlécértékkel le lehet csökkenteni a vaklármák számát.

Amennyiben a fenti módszerrel nem lehet a fájlokat visszavésni, akkor lehetőség van a technika további finomítására, azaz, rendelkezésünkre állnak a következő módszerek:

- **Töredék helyreállítás**: az eredeti fájl vagy beágyazott objektum két vagy több töredékét próbáljuk meg összeilleszteni.
- **Blokk alapú vésés**: a fájlokat blokkonként próbáljuk meg összerakni, feltételezve, hogy az adat nem töredezett, valamennyi egymást követő blokk egy logikai egységhez (egy fájlhoz, vagy egy beágyazott objektumhoz) tartozik.
- **Karakterisztika alapú vésés**: az adatokat a kódolási jellemzők (kódolási karakterisztika, entrópia) alapján vizsgáljuk, és így próbáljuk megkeresni az összetartozó fájlrészeket.
- **Fájlszerkezet alapú vésés**: a fájlokat az adatok belső szerkezetének részleges ismerete alapján próbáljuk meg helyreállítani – az eljárás alkalmazható például az ismert struktúrájú adatbázis fájlok esetén.
- **Szemantikus vésés**: a fájlokat a tartalom nyelvi/nyelvészeti elemzése alapján próbáljuk meg összerakni. Például magyar és angol szövegrészeket tartalmazó blokkok

[119] FAT tábla vagy inode.

egymásutánját vizsgálva megkeressük és összeragasztgatjuk az egymáshoz illő részeket.

- **Validációs vésés**: a fájlt nyers adatok alapján valamilyen speciális ellenőrző (validáló) szoftver segítségével kíséreljük meg helyreállítani, például a kódolás, illetve a kódolási lánc sajátosságainak messzemenő figyelembevételével.

Az egyes fájlok sikeres visszanyerését követően a visszavésett elemeket rekurzívan újra kell vizsgálni, hogy tartalmaznak-e további visszavéshető adatokat. Egészen addig, amíg meg nem győződtünk arról, hogy további adatok kinyerése már nem lehetséges. [63] [67] [68] [77]

II.2.3 A médiamenedzsment rétegben alkalmazott jellemző szoftver eszközök

A médiamenedzsment rétegben végrehajtott vizsgálatok zömét ugyan végre lehet hajtani nyílt forráskódú vagy ingyenes szoftverekkel, azonban ezeknek az eszközöknek az integrációja nem megoldott. A keresési, az elemzési feladatok végrehajtása, az eredmények értelmezése, konverziója és a laikus megbízó, hatóságok, bíróságok számára történő prezentációja körülményes. A „gyári" szoftverek ezzel szemben teljesen integráltak, több feladatot (adatvisszavésés, keresés, registry elemzés stb.) automatizáltak, a vizsgálatot végzőnek mindenekelőtt a feladatra és nem az eszközre kell koncentrálnia.

A legelterjedtebb információtechnológiai vizsgáló szoftverek:

- AccessData: **Forensics Toolkit**[120]**,**
- Guidance Software: **EnCase**[121]**,**
- X-Ways Software Technology AG: **X-Ways Forensics**[122]**,**
- Perlustro: **iLook**[123]**.**

[61] [71]

[120] L. http://accessdata.com/products/forensic-investigation/ftk

[121] L. http://www.guidancesoftware.com/

[122] L. http://www.x-ways.net/forensics/

[123] L. http://www.perlustro.com/

Az eltérő programok eltérő alapokra épültek: az X-Ways Forensics például egy hexaeditorból „nőtte ki magát”, az iLookot pedig az amerikai hatóságok kezdték el fejleszteni a nyomozati igények alapján. A különböző alapok hatása csak egy-egy funkció esetében érezhető[124]. Viszont elmondható, hogy a párhuzamos evolúciós fejlődés hatására napjainkban az egyes programok már funkcionalitásukat tekintve nagyon hasonlítanak egymásra, és komoly szolgálatot nyújthatnak az információtechnológiai eszközök elemzését végzőknek.

A fenti szoftvereket az informatikai törvényszéki vizsgálatok során nemcsak a médiamenedzsment réteg, hanem a megjelenítési és az alkalmazási réteg vizsgálata során is alkalmazzák, ezért a további két réteg leírása során ezeket már nem ismétlem meg ott.
Mivel a piacon elérhető forenzikus szoftverek rendkívül szerteágazó funkcionalitással rendelkeznek, ezért ezeknek a részletesebb ismertetésével értekezésemben nem foglalkozom.

II.2.4 A médiamenedzsment réteg által megkívánt szakmai kompetencia

A megjelenési réteghez köthető szakértői tevékenységek során adattárolási[125], feldolgozási[126] vagy adattovábbítási (számítógép-hálózati) adatstruktúrákat kell helyreállítani. Az ehhez szükséges kompetencia egyértelműen az informatikai szakterülethez köthető. Úgy vélem, hogy a médiamenedzsment rétegben az egyszerű adattárolási egységek azonosítását, a keresések elvégzését rá lehetne bízni az általános bűnügyi technikusokra, mert ezek a tevékenységek a fizikai rétegbeli tevékenységekkel analóg módon jól szabványosíthatók megfelelő módszertani útmutató mellett. Ezzel szintén csökkenteni lehetne a bűnügyi költségeket.

[124] Az X-Ways Forensics az egyik leghatékonyabb az adatvisszavésés terén, a prezentáció terén viszont a Forensics Toolkit nyújtja a legkényelmesebb, leghatékonyabb funkciókat.

[125] Különböző adathordozók vizsgálata esetén.

[126] Memória, processzor vizsgálatakor.

II.3 Megjelenítési réteg

II.3.1 A megjelenítési réteg meghatározása

Brian Carrier vizsgálati rétegmodelljében a megjelenítési réteg helyett a fájlrendszer (File System) szerepel, ami a fizikai tárolókon található fájlok helyreállítását, azonosítását és elemzését jelenti, az elemzés által visszaadott érték pedig fájlobjektum. A rétegben elvégzett vizsgálat nem minden esetben értelmezhető, például beágyazott adatok, vagy „árva", a fájlrendszerhez nem tartozó digitális objektumok esetén. A kötet elemzésből következő, a fájlrendszer elemzéssel azonos szinten lévő feladatként említi a csereterület (swap) elemzést és az adatbázis-elemzést is, azonban ezek tartalmát nem definiálja. [62 pp. 7–8]

Véleményem szerint az eredeti fájlrendszer réteg fogalom kiterjeszthető valamennyi digitális objektumra, azaz minden fájlra, csereterületre, függetlenül annak kiterjesztésétől (típusától), (normál, törölt, véglegesen törölt vagy törlés után részlegesen felülírt) státuszától, illetve a fájlrendszerben saját bejegyzéssel nem rendelkező – például egy fájlba ágyazott, swap vagy particionálatlan lemezterületről helyreállított – adatra. Digitális objektumnak tekinthetők a fájlok tárolási egysége a szektor és a fájlok valós méretének a különbségeként előálló maradványterületek (slack space), amelyek korábbi fájlok részleteit vagy lemezműveletek eredményét tartalmazhatják. Digitális objektumnak tekinthetők továbbá a számítógép-hálózatból kinyert sértetlen és sérült adatcsomagok és a memória és a processzor által tárolt, feldolgozott folyamat és rendszeradatok is, mivel ezek szintén nem jelennek meg fájlrendszerben, azonban a forenzikus vizsgálatok során jelentős mennyiségű hasznos információval szolgálhatnak.

Mivel itt nem csak fájlok, hanem a memória, a hálózati adatok, beágyazott adatcsomagok, azaz fájlrendszer bejegyzéssel nem rendelkező digitális objektumok vizsgálatáról van szó, biztos, hogy nem lehet fenntartani a Brian Carrier által eredetileg adott fájlrendszer réteg nevet. Az ebben a rétegben történő tevékenységeknek a célja a digitális objektumok tartalmának az értelmezése is, vagyis itt történik meg a metaadatok, hálózati és protokollinformációk elemzése, az objektumtípus vizsgálata. A feltárt digitális objektumok – többek között a fejléc azonosítás, kódolás helyességének ellenőrzése miatt – már egyértelműen azonosításra kerülnek. A további vizsgálati rétegben elvégzett vizsgálatoknak ezért már nem kell az adatértelmezéssel, az absztrakt szintaktikai szerkezettel és helyességével foglalkoznia.

Ez a funkcionális leírás jelentős egybeesést mutat az ISO OSI hétrétegű számítógép-hálózati modelljének megjelenítési rétegében leírtakkal, ezért javaslom a megjelenítési réteg elnevezés alkalmazását.

II.3.2 A megjelenítési rétegben elvégzendő általános feladatok, tevékenységek

A megjelenítési rétegbeli vizsgálatok célja a digitális objektumok leltárának elkészítése, metaadatainak[127] és kódolásának a vizsgálata, a hálózati adatok elemzése, azaz az adatkeretek belső szerkezetének feltárása, protokollinformációk dekódolása[128] és az átvitt adatok[129] információvá történő átalakítása, a hálózati események időbeli sorrendjének rekonstruálása.

A metaadatok lehetnek fájlrendszer és fájlszintűek. A fájlrendszer szintű metaadatok vagy közvetlenül a fájlbejegyzésekhez kapcsolódnak, mint az NTFS esetén a fájl kiterjesztés, a készítési (created), módosítási (modified) és utolsó hozzáférési (last accessed) dátum és időbélyegek, fizikai és logikai méret, vagy csak közvetve – a fájlbejegyzéseken kívül – kapcsolódó adatok, mint az Alternatív Adatfolyam[130] (ADS – Alternate Data Stream), vagy a Registry adatbázisban eltárolt bejegyzések[131].

Metaadatokat azonban nemcsak az operációsrendszer, hanem az egyes alkalmazások is rögzíthetnek. Az ilyen metaadatokat a fájlok a fájlstruktúra részeként de a felhasználó előtt rejtetten vagy csak speciális funkciók felhasználásával lehet elérni. Ilyen metaada-

---

[127] A metaadat az adattal kapcsolatos adat.

[128] Azaz az adatkapcsolati, hálózati, szállítási és alkalmazási rétegbeli protokollhierarchia „visszafejtése”.

[129] Ilyen adatok lehetnek email, dokumentumok, felkeresett weblapok, távoli rendszerekben kiadott parancsok, programok stb.

[130] Az ADS alkalmazása során egy fizikai állományhoz egy vagy több állományrészt lehet csatolni úgy, hogy közben az eredeti fájl mérete és egyéb fájlbejegyzés adatai nem változnak meg. Ezek a bejegyzések menedzselhetők a Windows beépített parancsaival, például a „notepad ártalmatlan.txt:rejtett.txt” parancsal létrehozható, megtekinthető és módosítható a „rejtett.txt” nevű szövegtípusú ADS. Azonban a felhasználó vagy rendszergazda által nem ismert ADS-ek azonosítása és kezelése csak speciális programmal lehetséges, aminek nem része a Windows telepítő.

A Windows többek között az internetről letöltött fájlok esetében egy „Zone.Identifier” ADS-ben tárolja a letöltés forrását (`URLZONE_INTRANET = 1`; `URLZONE_TRUSTED = 2`; `URLZONE_INTERNET = 3`; `URLZONE_UNTRUSTED = 4`). Ezért „tudja” az operációsrendszer, hogy a fájlt nem megbízható forrásból törlöttük le, és ezért kérdez rá elindítás előtt: biztosak vagyunk-e abban, hogy futtatni szeretnénk.

Az ADS-t a rosszindulatú kódok és felhasználók is felhasználják arra, hogy adatokat, programokat elrejtsenek az avatatlan szemek elől.

[131] A Registry tartalmazza például az utoljára futtatott programokat: az ún. `MRU` (Most Recently Used) kulcsokhoz tartozó adatok közt.

tokra példa a Microsoft Office által a Word, Excel Powerpoint stb. fájlokba rögzített felhasználó név, szervezet, számítógépnév és egyéb adat[132] vagy a különböző képekbe[133,134] integrált adatok, amelye többek között tartalmazzák a kép készítésének idejét, a készítésre felhasznált kamera típusát, illetve – amennyiben a digitális fényképezőgép (vagy okostelefon) tartalmaz GPS modult, úgy tartalmazza a kép készítésének helyét is (geotagging).

A megjelenítési rétegben elvégzendő feladatok között alkalmazható a médiamenedzsment rétegben ismertetett adat-visszavésési technika, amely során az azonosított digitális objektumokba ágyazott további digitális objektumok helyreállítására kerül sor. Az így kapott digitális objektumokon belül a visszavésés segítségével rekurzívan további digitális objektumok állíthatók elő.

A médiamenedzsment rétegben azonosított digitális objektumokat meg kell vizsgálni, azaz:

- fel kell tárni a digitális objektumok belső szerkezetét,
- dekódolni és elkülöníteni kell az egyedi- és a típusfüggő információkat,
- ki kell nyerni az egyes digitális objektumtípusra jellemző metaadatokat,
- ki kell nyerni a szöveges, illetve szövegként értelmezhető információkat,
- meg kell határozni az események sorrendjét, illetve az egymással valamilyen kapcsolatban lévő adathalmazokat,
- azonosítani kell a beágyazott digitális objektumokat.

[70] [76] [77] [78] [79]

Számítógép-hálózati adatok esetén szükséges az adatkeretek azonosítása és szétválasztása, mert ennek eredményeként lehet az adatcsomagokra épülő protokollkeret információit[135] értelmezni, és felhasználni azokat a hálózati adatforgalom dekódolására.

---

[132] L. http://office.microsoft.com/en-us/excel-help/find-and-remove-metadata-hidden-information-in-your-legal-documents-HA001077646.aspx

[133] L.: http://www.exif.org/specifications.html

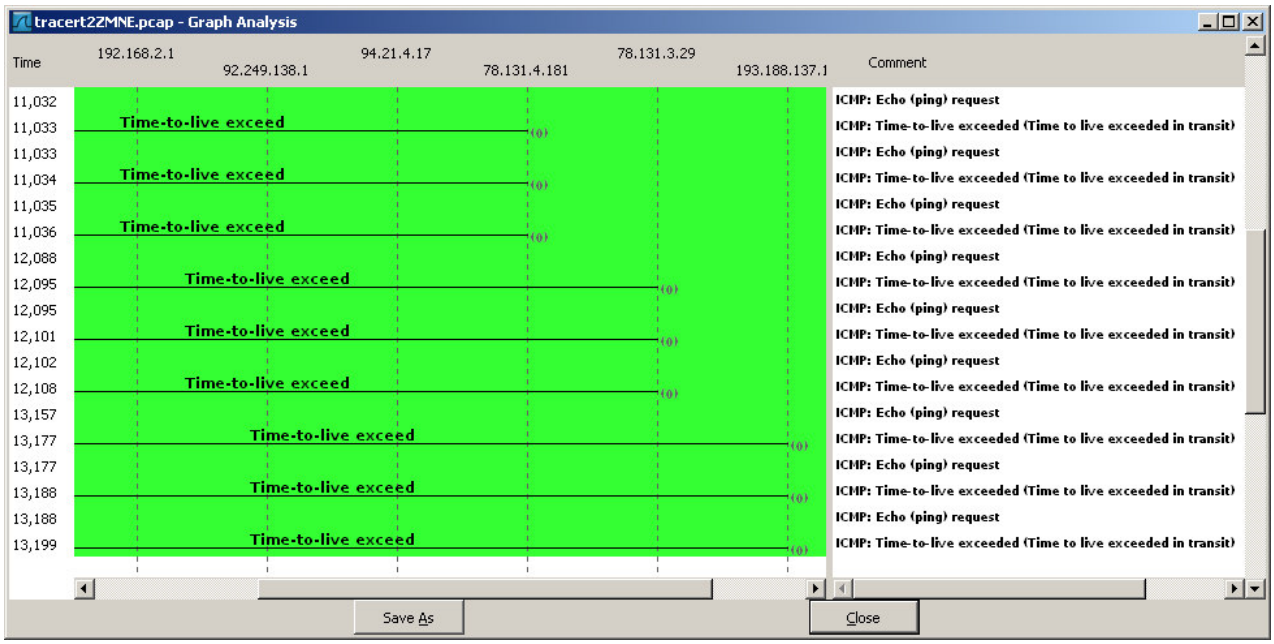
[134] A Microsoft Office bármely programjával készített adatok – egyéni beállítások vagy speciális metaadat eltávolító programok használatának hiányában – mindig tartalmazzák a készítő vagy módosító felhasználóhoz kapcsolható GIUD (Global Unique Identifier – globálisan egyedi azonosító) értékét. A GIUD generáláshoz az operációsrendszer felhasználja a hálózati kártya MAC címét is. Ennek felhasználásával tudták az „I love you” vírus készítőit is azonosítani.

[135] Vezérlő információk, sorszámok, hibajelző és hibajavító kódokat, időbélyegeket, IP, MAC címeket stb.

A hálózat adataival kapcsolatban a médiamenedzsment rétegbeli vizsgálatok eredményeként állnak elő a következő adatok:

- kapcsolat diagram → egymással kapcsolatban álló eszközök kapcsolathálója,
- esemény diagram → hálózati események és időzítésük,
- tevékenység diagram → felhasználói parancsok és időzítésük,
- protokoll lista és protokoll hierarchia,
- hálózati adatforgalmi statisztika,
- küldött és fogadott adatok.

A hálózati események elemzésre mutat példát a 20. ábra, ami egy hálózati útvonal felderítő (tracroute) parancs kiadását követő ICMP csomagküldési/fogadási folyamatról készült, illetve az ebben résztvevő IP útválasztókról ad információt.



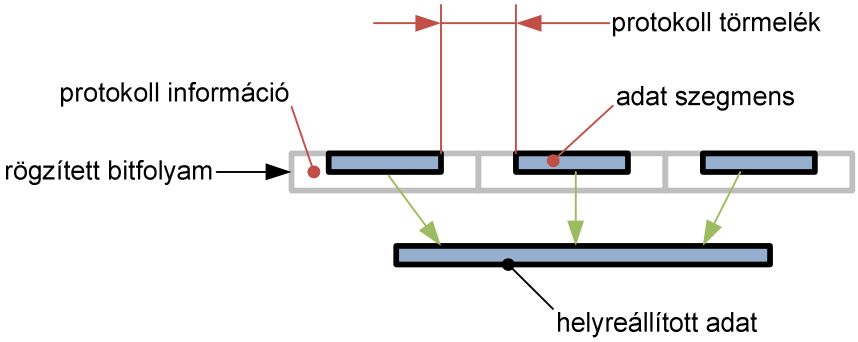
22. ábra – IP útválasztók sorozatát feltérképező traceroute parancs ICMP csomagjainak folyamat diagram részlete (szerk.: Illési Zsolt)

Amennyiben a megjelenítési réteg vizsgálatakor a médiamenedzsment rétegből kinyert keretek magasabb szinten helytelen értelmezéshez vezetnek, úgy vissza kell térni az elő-

ző rétegben definiált feladatok elvégzéséhez, valamilyen más megközelítést[136] keresve új adatkeretek előállításához.

Előfordulhat az is, hogy többszörös kísérletezés ellenére sem állítható elő a bitfolyam alapján egy helyesen értelmezhető adatkeret folyam. Ebben az esetben szintén a korábban már ismertetett adatvésési technikát lehet alkalmazni a protokollinformációk, vagy küldött/fogadott adatok helyreállítására. [68] [80]

A hálózati adatforgalom esetén az adatvisszavésés (l. 23. ábra) sajátos nehézsége a hálózaton küldött/fogadott adatok keretinformációi miatti adattöredezettség, a protokoll törmelék azonosítása és eltávolítása az adatok helyreállítása során. Ezt szemlélteti a következő ábra:



23. ábra – Adatvésés hálózati adatfolyamból
(szerk.: Illési Zsolt)

A megjelenítési réteg egyik sajátos részterülete az azonosított digitális objektumok hitelességének, eredeti/módosított/hamis voltának értékelése. Kriptográfiai hitelesítő adatok hiányában ez információ és kódelméleti elemzése alapján, a metaadatok és a fájl egyéb adatainak összevetésével, vagy a vizsgált adatfájl belső statisztikai elemzésével végezhető el.

Ide tartozik még az adatfájlok és a fájl belső jellemzőinek elemzése[137], az adatfájlok entrópiájának vizsgálata, így a rejtett és a titkosított adatrészek azonosítása. Ezt – egymásba ágyazott adatrejtést feltételezve – rekurzívan is el kell végezni.

A megjelenítési réteg elsősorban információ és kódelméleti és informatikai felkészültséget igényel, de speciális hálózati alkalmazások adatforgalmának elemzéséhez szükség le-

[136] Például más protokollbázist, más kezdőpontot alapul véve.

[137] A fájlok kiterjesztésének és a fájlok kódolásának összevetése.

het programozói, vagy az alkalmazás működésével kapcsolatos egyedi szaktudásra. [62] [63] [68] [80]

A megjelenítési rétegbeli vizsgálatok során elemezni lehet továbbá a(z)

- adatok kódolásának és kiterjesztésének az összhangját,
- esetleges titkosítását[138].

[71]

Ebben a rétegben történhet meg először az eredeti (másolat), hamisított vagy módosított adatok azonosítása és analízise, amennyiben ezt a fájlszerkezet és a kódolás lehetővé teszi.

A megjelenítési rétegben végrehajtott vizsgálatok során lehet elvégezni a digitális objektumok hash értékének a meghatározását és az így nyert értékek összehasonlítását nemzetközi vagy saját hash adatbázisokkal (például ismert jó/kártékony tartalmú fájlok); azonban sajnos jelenleg nincs olyan hash adatbázis, ami a kimondottan magyar vonatkozású szoftveradatokat, illetve a hazai gyakorlatban fellelt jogsértő tartalmak adatait tartalmazná. [81]

Ehhez a réteghez kötődik az szöveges információk keresése a szövegként értelmezhető tartalmú digitális objektumokban is. A keresésnek alapvetően két formája létezik:

- kulcsszavas keresés,
- mintaillesztéses keresés.

[71]

A kulcsszavas keresésnél az ügy szempontjából releváns szavakat vagy szótöredékeket keres a szakértő. Keresni lehet közvetlenül a digitális objektumokban, vagy azok elő-feldolgozásával készített index adatbázisban. Az index adatbázist a keresés előtt – a hatékonyság és a sebesség növelése érdekében – előre kell elkészíteni leindexelve valamennyi, a vizsgálatba bevont fájlokban található és szóként értelmezhető adatrészletet. Ez főleg akkor alkalmazható, ha várhatóan nagyon sok szóra, szórészletre kell rákeresni, illetve akkor, amikor nem egyértelmű az ügy kivizsgálásakor, hogy pontosan mit is kell ke-

[138] Ez a gyakorlatban az entrópia vizsgálatát jelenti.

resni[139]. Ilyenkor a vizsgálatot végzőnek tüzetesen és széles kulcsszó-bázist felhasználva kell az elkövetésre utaló nyomokat azonosítani.

A mintaillesztéses keresés során nem kötött adattartalmat, hanem egy ismert struktúrát kell keresni. Ilyen lehet a dátum, bankkártya szám, e-mail cím stb. A mintaillesztés során reguláris kifejezéseket (RegEx) kell készíteni, amelyek a keresett minta sajátosságait általános formában írják le. [60] [71]

A RegEx kifejezésekkel a probléma az, hogy komplex mintás keresésekor vagy nagyon sok hibás találatot hoznak fel (fals pozitív hiba), vagy nem találnak meg minden a keresendő mintára illeszkedő kifejezést (fals negatív). A 24. ábrán két e-mail formátumot kereső RegEx látható, azonban ezek a vizsgálat során sok olyan találatot eredményeznek, mi valójában nem e-mail cím. A hibás találatok kiszűrése – a RegEx jóságának függvényében – jelentős többletmunkát, többletköltséget generálhat.

a) `[\w-.]+@[\w-.]+`

b) `(?![ ])(\w|[.])*@(\w|[.])*`

24. ábra – Két rövid, e-mail formátumot kereső, de sok hibás találatot adó RegEx (szerk.: Illési Zsolt)

A megoldás lehet például a 25. ábrán is látható bonyolultabb kifejezés. A komplex RegEx ugyan a 24. ábrán láthatóakhoz képest pontosabb eredményt ad, azonban ezt a hosszú kifejezést a jelenleg használatos forenzikus szoftverek[140] nem tudják kezelni.

[139] Például a forgalom jelentős visszaesése miatti üzleti titoksértés gyanúja esetén a vizsgálat kezdetekor nem biztos, hogy ismert az elkövető, a kiszivárogtatott információt hasznosító konkurens cég(ek) neve(i), még a kiszivárogtatott adatok köre is bizonytalan lehet.

[140] Például az Encase, az FTK vagy az X-Ways Forensics.

```
(?:[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-
]+)*|"(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]|\\[\x01-
\x09\x0b\x0c\x0e-\x7f])*")@(?:(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\.)+
[a-z0-9](?:[a-z0-9-]*[a-z0-9])?|\[(?:(?:25[0-5]|2
[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4]
[0-9]|[01]?[0-9][0-9]?|[a-z0-9-]*[a-z0-9]:
(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-
\x7f])+)\])
```

25. ábra – Az RFC 2822-ben rögzített e-mail formátumot kereső komplex RegEx (forrás: [82])

[83]

A fenti reguláris kifejezéseket egy levelező szerver 226 MB-os naplóállományán tesztelve megállapítottam, hogy az

- 1. kifejezés (l. 24. ábra /a) 21 231 különböző e-mail címet azonosított, 2 164 552 különböző helyen,
- 2. kifejezés (l. 24. ábra /b) 20 456 különböző e-mail címet azonosított, 2 171 523 különböző helyen,
- 3. kifejezés (l. 25. ábra) 22 382 különböző e-mail címet azonosított, 2 158 623 különböző helyen.

A reguláris kifejezések keresési jóságát vizsgáló elemzésemben résztvevő valamennyi mintaillesztési kifejezés hibás. A keresés eredményeként visszaadott e-mail címként nem értelmezhető értékeket[141], illetve minden kifejezés figyelmen kívül hagyott[142], esetleg a levélcímhez nem tartozó karaktereket[143] is hozzákapcsolt a címhez.

A fentiek alapján megállapítottam, hogy az egyes szoftverek reguláris kifejezéseinek szintaxisa eltérő, a kezelhető kifejezések hossza korlátozott, az egyes szoftverek fejlesztői által javasolt keresési minták nem hasonlíthatók össze, és nincs egységes szakmai

[141] A mintaillesztéses keresés visszaadta például az alábbi nem e-mail-cím értékeket:
1: `-@teszt.hu`;
2: `000000@email`;
3: `#public@teszt.hu`.

[142] A keresés például nem adta vissza a következő értékeket:
1: `1edasc4onspur0slzcv2s1v1mcbohf63-b@news.quickoffice.com`;
2: `22098@webreply.marketingszoftverek.hu`;
3: `102827@runcdfirst.bitandpixel.hu`.

[143] Például a naplózó szoftver által az email cím elé írt „=” karaktereket.

standard az egyes keresések eredményének összehasonlítására. Tudományosan megalapozott keresési módszerek hiányában az elsőfajú hiba és a másodfajú hiba aránya nem ismert, így a jelenlegi módszerek alkalmazása a büntetőeljárásban – ha nem is szakszerűtlen, de – nyilvánvalóan megkérdőjelezhető.

II.3.3 A megjelenítési réteg által megkívánt szakmai kompetencia

A megjelenítési réteggel kapcsolatos feladatok, amennyiben nyilvánvalóan nem törölt, nem módosított adatokat kell a vizsgálatba bevonni[144], általános informatikai képzettséget igényelnek. Ezek a feladatok könnyen és jól általánosíthatók, illetve a piacon rendelkezésre álló, az információtechnológiai rendszerek vizsgálatát támogató forenzikus szoftverek jelentős támogatást nyújtanak az elvégzésükhöz. Ezért – megfelelő módszertani útmutató birtokában – az általános feladatokat szintén elvégezhetik az általános bűnügyi technikusok.

Meg kell jegyeznem azt, hogy amíg a fizikai réteghez köthető feladatok a gyakorlatban is egységesen kezeltek, a megjelenítési rétegben végzett tevékenységek már jelentős eltéréseket mutatnak, attól függően, hogy a végrehajtás során milyen programokat és milyen módszertanokat alkalmaznak. Amint azt fentebb már említettem, például az adatvisszavésést eltérő paraméterek és eltérő szintaxis mellett kezelik a forenzikus szoftverek. A gyakorlati tesztek alapján egyértelmű, hogy a különböző programok különböző eredményeket adnak azonos vizsgálati adatok esetén. A tapasztalati különbségek nem lényegesek, az viszont zavaró, hogy nem ismert az egyes programok hibaaránya, az elsőfajú és a másodfajú hibák szignifikancia szintje, illetve nincs olyan teszt adatbázis és tesztelési módszertan, ami az egyes eszközök eltérő eredményeinek tudományos alaposságú elemzését lehetővé tenné validációs, illetve kalibrációs tesztek formájában. Ez egy olyan kutatási terület, amivel az információtechnológiai krimináltechnika művelőinek a jövőben mindenképp foglalkozniuk kell, hogy a vizsgálatok maradéktalanul megfeleljenek a Daubert kritériumoknak.

A keresések, a hibákkal kapcsolatban leírtak alapján magasabb szintű, mérnöki informatikai szakértői kompetenciával végezhetők el. Magasabb információtechnológiai –

[144] Ilyen feladatok például a hash-elés, a fájl kiterjesztés és a kódolás összevetése, a fájlok egyszerű kimásolását igénylő feladatok, metaadatok kinyerése.

igazságügyi szakértői – kompetenciát igényel az adatrejtés felfedése, a titkosítások megfejtése.

II.4 Alkalmazási réteg

II.4.1 Az alkalmazási réteg meghatározása

Brian Carrier vizsgálati rétegmodelljében az alkalmazási réteg (Application) alapvetően a digitális objektumként visszanyert adatok értelmezésével kapott adat elemzését és értékelését jelenti. [62 pp. 7–8]

Véleményem szerint az alkalmazási réteg fogalma megfelelő, amennyiben ideértjük a kódok elemzését, értelmezését is.

II.4.2 Az alkalmazási rétegben elvégzendő általános feladatok, tevékenységek

Az alkalmazási réteggel kapcsolatos feladatok célja a hálózati és tárolási protokollinformációktól megtisztított adatok értelmezése, büntetőjogilag releváns információ kinyerése. Az alkalmazási rétegbeli vizsgálatok tárgya lehet informatikai, információtechnológiai jellegű, például az adatfájlok metaadatainak feltárása, az adatokban található SQL, shell stb. parancsok értelmezése, programok visszafejtése, a kódlogika értelmezése a vizsgált cselekménnyel kapcsolatban. [60] [70] [75]

Ebben a vizsgálati rétegben már olyan egyéb – nem információtechnológiai vagy számítógép-hálózati jellegű – adat is megjelenik, ami meghaladja az informatikai igazságügyi szakértő kompetenciáját. Fénykép jellegű digitális objektum esetén megállapítani az azon szereplő személy életkorát igazságügyi orvosszakértői feladat. Szerzői védelem alá eső adatok[145] elemzésekor az okozott anyagi hátrány megállapítása, vagy egyes esetekben a szerző, előadó azonosítása speciális, nem információtechnológiai szakértelmet és szakértői jogosítványokat kíván; így az ilyen adatokat tartalmazó ügyeket érdemben

[145] Program-, kép-, hang- és videófájlok.

együttes, vagy egymást követő kirendelésekkel lehet szakszerűen lefednie a nyomozóhatóságoknak[146]. [67]

Az alkalmazási rétegben lévő vizsgálatok, lehetőségek száma, az értelmezésbe bevonható szakterületek száma majdnem akkora, mint ahány alkalmazás létezik, így ezeknek a részletes feltérképezése, modellezése eddig még nem történt meg, és a módszertani feladatok szisztematikus azonosítása és szabványosítása a közeljövőben nem is várható.

II.4.3 Az alkalmazási réteg által megkívánt szakmai kompetencia

A fent leírtak alapján az alkalmazási réteg feladatai annyira sokrétűek, hogy jelen értekezés terjedelmében nem határozható meg egyértelműen az ebben a rétegben végrehajtandó tevékenységeknek a köre.

Informatikai szakkérdés az adatok megjelenítése, „tálalása", kinyerése és esetleges átkódolása a többi szakterület szakértői számára, illetve „programozott problémák" értelmezése, minden egyéb feladathoz az ügy jellegéhez, a releváns kérdéshez külön-külön kell a kompetenciaterületet meghatározni.

[146] Például az informatikai igazságügyi szakértő feltárja a terhelt által küldött-fogadott képeket, amelyeket ezután igazságügyi orvosszakértő elemez.

Következtetések

A rétegmodellel kapcsolatos kutatásaim alapján megállapítottam, hogy az információtechnológia krimináltechnikai vizsgálatai egységes szerkezetben jól kezelhetők Brian Carrier modelljének az általam tett kiegészítéseivel. **Igazoltam, hogy az eredeti rétegmodell csak a vizsgálatok részhalmazára[147] alkalmazható**, nem tartalmazza az elvégezhető tevékenységek rendszerét és kapcsolódásait, illetve nem foglalkozik az egyes rétegekben elvégzendő funkciók ellátásához szükséges szakmai kompetenciákra sem. **Az általam javasolt** kiegészített **modell** egyes rétegei az informatikában több területen is alkalmazott **absztrakciós rétegek segítségével teszik lehetővé a szakértői vizsgálatok komplex rendszerének leegyszerűsítését, az egyes tevékenységek kapcsolatának leírását, illetve a szükséges kompetenciák azonosítását**.

Az absztrakciós réteg kidolgozásakor **összesítettem és rendszereztem** az alábbiak szerint **az informatikai szakértői fő tevékenységeket az absztrakciós rétegek tükrében**:

TEVÉKENYSÉG	**VIZSGÁLATI RÉTEG**
adathordozók mentése	fizikai réteg
hálózati adatforgalom mentése	fizikai réteg
törölt fájlok helyreállítása	médiamenedzsment réteg
formátum konverzió	médiamenedzsment réteg
beágyazott, sérült, rejtett stb. fájlok rekurzív keresése és rekonstrukciója	médiamenedzsment réteg
hash értékek kiszámítása	megjelenítési réteg
jellemző adatok keresése (osztály és alosztály jellemzők, egyedi hardver, szoftver eszközre, személyre jellemző adatok keresése)	megjelenítési réteg
jelszavak helyreállítása	megjelenítési réteg
keresés (kulcsszavas és mintaillesztéses)	megjelenítési réteg
kódolás kiterjesztés összevetése	megjelenítési réteg
összehasonlítás ismert adatokkal (bit-bit összehasonlítás, hash értékek keresése, „digitális DNS” alapú összehasonlítás)	megjelenítési réteg

[147] Azaz nem kizárólag az adathordozókkal kapcsolatos tevékenységekre.

TEVÉKENYSÉG	VIZSGÁLATI RÉTEG
szűrés (a vizsgálandó adatmennyiség redukálása, az ismert fájlok/ objektumok eltávolítása az elemzendő mintából)	megjelenítési réteg
titkosított adatok megfejtése	megjelenítési réteg
eredetiség vizsgálat	megjelenítési réteg[148] alkalmazási réteg[149]
tranzakciók dátum és időadatainak keresése és idősorok összeállítása	megjelenítési réteg[150] alkalmazási réteg[151]
adatbányászat[152]	alkalmazási réteg

2. táblázat – Informatikai szakértői fő tevékenységek az absztrakciós rétegek tükrében (szerk: Illési Zsolt)

[148] A kódolási jellemzők vizsgálati része tartozik ehhez a réteghez – főleg a másolat, vagy a módosított fájlok/adatok azonosítására.

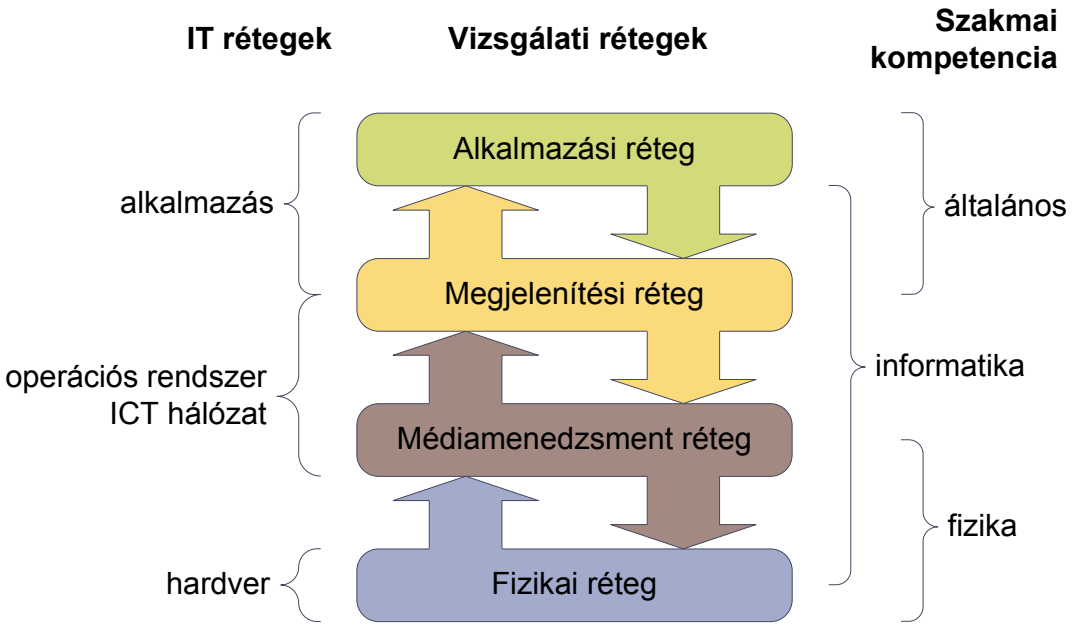
[149] A fájl adatainak értelmezésével (információtartalmának elemzésével), főleg a hamisított fájlok/adatok azonosítására. Ez a feladat esetenként egyéb szakterületi szakértők bevonásával oldható meg.

[150] Fájlrendszer szinten és fájl-metaadatokban tárolt dátum és időadatok kinyerése és értelmezése.

[151] Az adatok értelmezésével (információtartalmával) kinyert dátum és időadatok.

[152] Az adatbányászat a kriminálinformatikával határos terület.

Az **absztrakt rétegmodellnek** egy másik, az egyes rétegek tevékenységeinek kapcsolatát, a vizsgálandó információtechnológiai komponensek és a szakmai kompetenciákat **összefoglaló modelljét is megalkottam az alábbiak szerint**:



26. ábra – Információtechnológiai rendszerek vizsgálati rétegei (forrás: Illési Zsolt)

A vizsgálataim alapján **megállapítottam, hogy a keresés jellegű műveletek**[153] jelenleg alkalmazott **módszereinek nem ismert a hibaaránya, nincs egységes és kiforrott a módszertana**, ezért javaslom ezek tudományos alaposságú kutatását – az ilyen jellegű tevékenységek valós természetének megállapítása érdekében.

[153] Visszavésés, szó és kifejezés keresés, mintaillesztés.

III. INFORMÁCIÓTECHNOLÓGIAI KÖRNYEZETHEZ KAPCSOLÓDÓ KRIMINÁLTECHNIKAI TEVÉKENYSÉGEK MODELLEZÉSE

A bűnüldöző szervek, a nyomozóhatóságok és a bíróság a büntetőeljárás során többször kerülnek olyan helyzetbe, amikor a tényállás egyes elemeinek értelmezéséhez nem elegendő az általános műveltség, hanem sajátos felkészültség és ismeret szükséges. Ezt a speciális szakmai ismeretet biztosítják a Magyar Igazságügyi Szakértői Kamara (a továbbiakban: MISZK) tagjai az eljáró hatóságok számára. Az eljáró igazságügyi szakértőkkel és a feladataikkal kapcsolatban a jogszabályok[154] részletesen meghatározzák, hogy kik milyen módon végezhetik a tevékenységüket.

Informatikai igazságügyi szakértőként azt tapasztalom, hogy a büntetőeljárások mindennapi gyakorlatában informatikai és igazságügyi jellegű szakértői kompetenciát igénylő feladatokat nem igazságügyi szakértők[155] is ellátnak, illetve az informatikai igazságügyi szakértők munkája a végzettségük, szakmai tapasztalatuk és eszközparkjuk függvényében jelentős szakmai és minőségi eltérést mutat. A szakvélemények heterogenitása, minőségi különbségei azért jelentenek problémát, mert azok esetleges fogyatékosságai miatt az ügydöntő hatóság a tényállást nem tudja helytállóan megállapítani, utólagosan rekonstruálni. Ebből kifolyólag előfordulhat, hogy a sértettek nem nyernek megfelelő elégtételt és kártérítést, a bűnösök nem kapnak megfelelő büntetést. A szakvélemények hibája miatt előfordulhat pont az ellenkezője is: sértettként lehetnek azonosítva, és kártérítést kaphatnak arra jogosulatlanok, és bűnösként lehetnek elítélve akár ártatlanok is.

A szakvélemények általános hibái a következők lehetnek:

- **kompetencia megsértése** – azaz a jogkérdésben nyilvánított vélemény, a kirendelő határozatban fel nem tett kérdésre adott válasz[156] és a leleten kívül található forrásból származó bizonyítékokra tekintettel adott szakvélemény,
- **tartalmi megalapozatlanság** – azaz az iratellenesség, téves következtetés, hiányzó ténymegállapítás és felderítetlenség,

[154] A szakértői tevékenységről szóló 2005. évi XLVII törvény, az igazságügyi szakértői kamaráról szóló 1995. évi CXIV. törvény, az igazságügyi szakértői működésről szóló 31/2008. (XII. 31.) IRM rendelet stb.

[155] Például a hatóságok munkatársai vagy az eseti szakértők.

[156] Álláspontom szerint ilyennek kell tekinteni a kirendelő határozatokban gyakran előforduló „a szakértő egyéb észrevételei" jellegű formulákra adott, az érdemi kérdések keretén túlmutató válaszokat is.

- **módszertani megalapozatlanság** – azaz a szakértő a szakvéleményben nem, vagy értékelhetetlen sekélyességgel jelöli meg a vizsgálat módszerét és annak validitását. [41 p. 136]

Meg kell említenem, hogy a módszertanok bizonytalanságai nem általánosak a MISZK szakértői körében. Vannak olyan igazságügyi szakmai részterületek[157], amelyekre az a jellemző, hogy képviselői egységes módszertani elvek alapján végezik a tevékenységüket. Ez az egységesség és módszertani megalapozottság azonban egyáltalán nem a MISZK érdeme, hanem a fenti szakterületeket képviselő kamarák[158] színvonalát és több évtizedes szakmai munkáját dicsérik.

A minőségi eltérések mellett jellemző az is, hogy informatikai kérdésekben a kirendelő/megbízó hatóság az információtechnológiai szakmai kompetencián túlmutató kérdésekre is választ vár[159].

Véleményem szerint az informatikai szakvélemények szakmai színvonalának emeléséért rengeteget kellene és lehetne tenni, ennek megvannak mind a szakmai, mind a módszertani alapjai. A módszertani levelek lehetőséget biztosítanának a büntetőeljárásban a kirendelő hatóságok laikus tagjainak arra is, hogy egy szakmai katalógusra épülve szakszerű kérdéseket tegyenek fel, illetve a módszertani levelek segítenek abban is, hogy a laikusok értelmezni is tudják a kérdéseikre adott szakmai válaszokat.

A következőkben áttekintem a szakszerűségét meghatározó legfőbb jogszabályi követelményeket, modellezem a büntetőeljárás szakaszait és azok kapcsolatát, áttekintem és modellezem a szakértői szerepeket és feladatokat, illetve elkészítem a vizsgálatoknak a krimináltechnikai szempontból egyik legfontosabb szakaszának – a helyszínen végzett nyomfelkutatási, -biztosítási és -rögzítési tevékenységeknek – az egységesített fizikai és digitális kriminalisztikai tevékenységmodelljét.

[157] Igazságügyi orvostan, közúti közlekedésbiztonsági műszaki, igazságügyi könyvszakértő stb.

[158] Magyar Orvosi Kamara, Magyar Mérnöki Kamara és a Magyar Könyvvizsgálói Kamara.

[159] Például szerzői jogsértések esetén az okozott kár, a károsult azonosítása vagy a jogsértés meglétének megállapítása.

III.1 Információtechnológiai vonatkozású kriminálltechnikai tevékenységek szakszerűsége

A hagyományos, csak fizikai helyszínnel rendelkező bűncselekmények helyszíni cselekményeivel kapcsolatban jól kidolgozott és kipróbált protokollokat alkalmaznak az eljáró hatóságok. Az információtechnológiai eszközöket, hálózatokat is tartalmazó „virtuális helyszínnel" is rendelkező ügyekben a kép ezzel szemben már nem ilyen letisztult.

A hagyományos helyszíni vizsgálatok során a helyszín egyértelmű, a filmekből jól ismert sárga-fekete szalaggal körbehatárolható. Az információtechnológiai elemeket is tartalmazó helyszín a csupán fizikai nyomokat tartalmazóval ellentétben több virtuális elemet is tartalmaz (például internet). Ez a széttagoltság megnehezíti, sőt lehetetlenné teszi a körbekerítést, a virtuális helyszínen található valamennyi helyiség, ember, eszköz kontrollját. A vizsgálatot végző hatóság tagjainak – de sokszor még a tapasztalt informatikai szakembereknek is – nehézséget okozhat, hogy valamennyi olyan eszközt azonosítani tudjanak, amelyik digitális adatokat tárol vagy továbbít.

A kezdeti lépések bizonytalanságát nagymértékben csökkenti, ha az azt végző szakemberek fel tudnak készülni a nyomrögzítéskor rájuk váró technikai eszközökkel való munkára, ha van előzetes képük arról, hogy mivel fognak szembenézni, illetve ha szisztematikusan térképezhetik fel, biztosíthatják és rögzíthetik a nyomokat, legyen szó akár fizikai nyomról[160] vagy digitális nyomról[161].

III.1.1 Szakértői módszertani levél

A szakértői módszertani levelekkel kapcsolatban három jogszabály határozza meg a megismételhetőség, a tudományos-technikai megalapozottság követelményeit és a szakértőkkel kapcsolatos szakmai kötöttségeket az alábbiak szerint:

[160] Anyagmaradvány, lenyomat.

[161] Adatmaradvány.

1) Az igazságügyi szakértői kamaráról szóló 1995. évi CXIV. törvény (a továbbiakban: Iszktv.) a módszertani levelekkel kapcsolatban kimondja, hogy

„A Magyar Igazságügyi Szakértői Kamara

16. § (2) A küldöttgyűlés

g) megalkotja a szakértői tevékenység etikai kódexét és az etikai eljárási szabályzatot, a szakértőjelölti igazolvány kiadásáról és külalakjáról szóló szabályzatot, valamint a szakértői módszertani levél kiadásának részletes szabályairól szóló szabályzatot." [84]

2) Az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény (a továbbiakban: Szaktv.) a szakértői módszertani levelekkel kapcsolatban a következőket állapítja meg:

Szakértői módszertani levél

„30/A. § (1) A MISZK elnöksége (a továbbiakban: elnökség) a szakértői tevékenység egységes és magas színvonalú ellátása érdekében szakértői módszertani levelet ad ki. A módszertani levél kiadását a MISZK és a szakértői kamara szakbizottságai, valamint a miniszter indítványozhatja.

(5) Az elnökség nem adhat ki szakértői módszertani levelet olyan szakterületen, amelyen az egészségügyért felelős miniszter vagy annak irányítása, felügyelete alatt működő szervezet külön jogszabály alapján módszertani levél kiadására jogosult.

30/C. § (1) A miniszter gondoskodik a szakértői módszertani levél Hivatalos Értesítőben történő közzétételéről, és az általa vezetett minisztérium honlapján való megjelentetéséről. A szakértői módszertani levél – annak visszavonásáig – a honlapról nem távolítható el.

(3) Az elnökség figyelemmel kíséri a közzétett szakértői módszertani leveleket, és szükség esetén intézkedik – a szakértői módszertani levél kiadására vonatkozó rendelkezések alapján – azok visszavonásáról, illetve új módszertani levél kiadásáról.

30/D. § A szakértői módszertani levél a Hivatalos Értesítőben történő közzétételétől a kirendelő szerv számára tájékoztatásul, a szakértőnek pedig a szakértő tevékenység ellátása során iránymutatásul szolgál. Ha a szakértő a szakértői módszertani levélben foglaltaktól eltér, azt a szakvéleményben meg kell indokolnia." [85]

3) A Be. közvetlenül ugyan nem hivatkozik a módszertani levelekre, de több helyen is megköveteli a résztvevőktől, hogy definiálják az általuk használt módszereket, illetve a módszerekkel és eszközökkel kapcsolatban sajátos követelményeket tesz:

*„**Szakértői vizsgálat***

105. § (1) A szakértő szakértői vizsgálat alapján ad véleményt. A szakértő a vizsgálatot a tudomány állásának és a korszerű szakmai ismereteknek megfelelő eszközök, eljárások és módszerek felhasználásával köteles elvégezni." [44]

Ez a bekezdés tulajdonképpen megfogalmazza a Daubert kritériumok alkalmazásának kötelmét, azaz: a jogalkotó megköveteli a tudományosan megalapozott szakvéleményt. A Be. további tartalmi követelményeket fogalmaz meg a szakvéleménnyel kapcsolatban:

*„**A szakvélemény előterjesztése***

108. § (2) A szakvélemény magában foglalja

b) a vizsgálat módszerének rövid ismertetését." [44]

Azaz: a szakvéleményt készítő szakértőnek nemcsak a következtetéseket kell leírnia, hanem az elvégzett vizsgálatokat is, hogy azok egy másik szakértő által is elvégezhetők és/vagy validálhatóak legyenek. Véleményem szerint a bekezdés alapján nemcsak egy szűkszavú leírást kell megadni a szakvéleményben, hanem az elvégzett vizsgálat teljes körű rekonstrukciójához szükséges adatokat, illetve le kell írni az esetleges logikai következtetés menetét, annak főbb állomásait is, hogy ellenőrizhető legyen a konklúzió érvényessége és igaz volta is.

A Be. További követelményeket is megfogalmaz a szakértői vizsgálatok egy részhalmazára a titkos adatszerzésre is, a következők szerint:

*„**Bírói engedély***

203. § (1) A titkos adatszerzés engedélyezéséről a bíróság az ügyész indítványára e Fejezet VI. Címe szerinti eljárásban határoz.

(2) Az indítványnak tartalmaznia kell

c) a titkos adatszerzés tervezett alkalmazásával érintett nevét, illetőleg az azonosításra alkalmas adatot, valamint a titkos adatszerzés vele szemben alkalmazni kívánt eszközének, illetőleg módszerének megnevezését,

e) az alkalmazás 201. §-ban és 202. §-ban meghatározott feltételeinek a meglétére vonatkozó részletes leírást, így különösen az alapul szolgáló bűncselekmény megne-

vezését és a bűncselekmény gyanújára okot adó adatokat, a titkos adatszerzés elkerülhetetlen alkalmazását indokoló körülményeket, az alkalmazás célját és annak valószínűsítését, hogy a bizonyíték a titkos adatszerzés során alkalmazott eszközzel, illetőleg módszerrel beszerezhető,

(4) A bíróság az indítvány előterjesztésétől számított hetvenkét órán belül határoz. Ha a bíróság az indítványnak helyt ad vagy részben ad helyt, meghatározza, hogy kivel szemben, a titkos adatszerzés mely eszköze, illetőleg módszere mettől meddig alkalmazható.

A titkos adatszerzés végrehajtása

204. § (5) A titkos adatszerzés végrehajtásáról jelentést (168. §) kell készíteni, amely részletesen tartalmazza a titkos adatszerzés lefolyását, így különösen azt, hogy annak során milyen eszközt, illetőleg módszert, meddig és hol alkalmaztak." [44]

A jogalkotó itt is azt az általános szakértőkkel szembeni követelményt fogalmazza meg, hogy az adatszerzést csak ismert eszközökkel é módszerekkel lehessen végrehajtani. Az adatszerzés – véleményem szerint – szakértői vizsgálatként is értelmezhető, mivel a titkos adatgyűjtés technikai feltételeinek végrehajtása (például számítógép-hálózat adatforgalmának lehallgatása), a begyűjtött adatok integritásának megőrzése speciális szakértelmet kíván, ezt a feladatot nem tudja bárki végrehajtani. Az általános szakértői vizsgálatokkal szemben itt a jogalkotó a vizsgálat előtt kell ismertesse indítványában az alkalmazni kívánt módszereket és eszközöket. Az engedélyező bíró így mérlegelheti egyrészt, hogy azok nem jelentenek-e túlzott beavatkozást a terhelt jogaiba, másrészt, hogy biztosítson megfelelő garanciális féket a nyomozóhatóság esetleges túlkapásaival szemben.

A szakértői módszertani levelek elkészítését a jogszabály csak a MISZK feladatává teszi, azonban a Be. rendelkezéseiből kiderül, hogy például a titkos adatszerzés során az azt végrehajtónak előre meghatározott módszerek és technikák alapján kell a feladatát elvégeznie.

A minisztériumok honlapján is csak itt-ott lehet szakértői módszertani leveleket találni; ezeknek a központilag egységes kezelése és publikálása nem megoldott, csak eseti módon történik.

Szakértői feladatokat[162] viszont nemcsak az igazságügyi szakértők, hanem esetenként az eljáró hatóságok tagjai is végeznek. Nevesített szakértői jellegű feladatkör a szaktanácsadói, akinek az igénybevételét a Be. 182.§ (1) bekezdése megengedi, ha a bizonyítási eszközök felkutatásához, megszerzéséhez, összegyűjtéséhez vagy rögzítéséhez különleges szakismeret szükséges.

Érdekesség, hogy amíg az igazságügyi szakértéssel és szakértővé válással kapcsolatban a jogszabályok szakmai szűrőket építettek be[163], addig az eljáró hatóságok szakértői jellegű tevékenységet végző tagjaival és a szaktanácsadókkal szemben ilyen követelményt a jogszabályok nem tartalmaznak[164].

III.1.2 Szakértők szakmai továbbképzése

A szakértői tevékenység minőségének javítását szolgálná a Szaktv. képzésekkel kapcsolatos fejezete is, amely kimondja a következőket:

*„**Az igazságügyi szakértők képzése***

18. § (1) Az igazságügyi szakértő részére szükséges jogi ismeretek oktatásának és a jogi vizsgának a megszervezéséről a miniszter gondoskodik. A rendszeres jogi oktatáson való részvétel és – a miniszter rendeletében meghatározott mentesülés esetét kivéve – az igazságügyi szakértő névjegyzékbe való felvételét követő jogi vizsga letétele kötelező.

(2) Az igazságügyi szakértő a névjegyzékbe való felvételéről szóló határozat kézhezvételétől számított 15 napon belül köteles a jogi oktatásra és a jogi vizsgára jelentkezni vagy a vizsga alóli mentesülési feltétel meglétét igazolni.

18/A. § Az igazságügyi szakértő számára kötelező a névjegyzékbe való felvételről szóló határozat kézhezvételétől számított egy éven belül a szakértés alapismereteivel összefüggő képzésben való részvétel és – a miniszter rendeletében meghatározott mentesülés esetét kivéve – az ehhez kapcsolódó vizsga letétele. Az alapismereti oktatásról és vizsgáról a MISZK gondoskodik, a vizsgát a mellette működő vizsgabizottság előtt kell letenni.

---

[162] Vagyis, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges. L. Be. 99. § (1) bekezdés.

[163] Ilyen speciális szűrő lehet a képesítés, a legalább ötéves szakmai gyakorlat, illetve a kötelező kamarai tagság. L. Szaktv. 3. §.

[164] A szaktevékenységeknek szakértői módszertani levelekhez való kötése ezen a területen is jelentős javulást hozna, mivel az eljáró hatóság „laikus szakértőivel" és a szaktanácsadókkal szemben is meghatározna legalább egy szaktevékenységgel összefüggő módszertani és eszköz minimumot.

18/B. § Az igazságügyi szakértő köteles a szakértői tevékenysége gyakorlásához szükséges rendszeres szakmai továbbképzésen részt venni, és a miniszter rendeletében előírt képzési kötelezettség teljesítését igazolni." [85]

A jogszabály alapján tehát jogi és szakmai képzéseket és vizsgákat is kéne szerveznie a MISZK-nek a minisztériumokkal karöltve. A jogi képzés valóban működik. Az igazságügyi szakértők a szakértéssel kapcsolatos ilyen irányú ismereteiket megszerzik, ebből vizsgáznak, és jobbára megoldott a továbbképzés, az ismeretek felfrissítése is. A szakmai felkészítés és vizsgáztatás azonban nem megoldott[165]. Nincsenek olyan – az igazságügyi szakértő és a hatóságok számára elérhető – szakmai zsinórmértékek, amelyek alapján egységes alapon értékelhető lenne az információtechnológiával kapcsolatos szakmai működés és az igazságügyi szakvélemények.

A jogszabályok elemzése alapján megállapítható tehát, hogy kötelező és szükséges lenne szakértői módszertani leveleket készíteni, de ezzel kapcsolatban informatikai téren nem történt semmi, a minisztériumok és a MISZK mulasztásos törvénysértést követnek el a módszertani levelek és publikálásuk hiányával.

III.2 Az információtechnológiai szakértés általános modellezése

A jogszabályelemzés tehát azt sugallja, hogy az igazságügyi szakértés módszertani keretei legyenek rögzítve, ezzel is biztosítva a büntető eljárásban résztvevők számára az optimális szakmai munkavégzés alapjait. Véleményem szerint a módszertani keretek megteremtésének az alapja egységes, modellszemléletű megközelítést kíván. A modellel kapcsolatban felmerül az, hogy egyszerre mutasson irányt a jogalkalmazóknak és az igazságügyi szakértőknek, tartalmazzon minden funkcionális igényt, ami a szakértéssel kapcsolatban jogi, informatikai vagy kriminalisztikai szempontból szóba jöhet. A korszerű funkcionális modellek azonos súlyt helyeznek a folyamatokra (eljárásokra) és az anyagi sza-

[165] Nincs olyan képzés hazánkban, ami az informatikai igazságügyi szakértés alapismereteivel függene össze. A probléma az, hogy olyan ismereteket egyetlen magyar felsőoktatási intézmény sem ad, amelyek az informatikai igazságügyi szakértés speciális követelményeivel foglalkoznának, nem ismertetik a rendelkezésre álló technológiákat, hardver és szoftver eszközöket, módszereket és technikákat. A hazai informatikai jogi/jogi informatikai oktatás egyik fellegvárának számító Pécsi Tudományegyetemen az információtechnológia kriminológiai ismeretei között csak a mátrixnyomtató lenyomatának elemzésével foglalkoznak.

bályokra. Ezek mellett a jó modell egyértelműen meghatározza az egyes feladatokban résztvevő szereplők körét és felelősségét. A modellezéssel kapcsolatban jogosan fogalmazható meg az a követelmény is, hogy az eredmények felhasználásával hatékony informatikai támogatás is kialakítható legyen. Meggyőződésem, hogy az igazságügyi szakértői levelek alapjául – a fenti követelmények maradéktalan betartása mellett – az UML modellezés az elérhető módszerek közül a legjobb. Ezért értekezésemben igazolni kívánom, hogy az üzleti folyamatok mintájára a büntetőeljárás, azon belül az igazságügyi szakértői feladatok is modellezhetők. Ennek alátámasztására – a terjedelmi korlátok miatt a modellezésnek csak egy részhalmazát kiemelve – osztálydiagramokat, állapotdiagramokat és használói esetdiagramokat készítek.

A modellezési bemutatóm során a következő főbb kérdések megválaszolását és modellezését demonstrálom:

- Hol értelmezett az informatikai igazságügyi szakértői tevékenység?
- Mik a bizonyítás eszközei és a bizonyítékok állapotai?
- Kik a büntetőeljárás szereplői, ezek közül ki vezet informatikai szakértés jellegű feladatokat?
- Mik a digitális nyomfelkutatás, -rögzítés, -biztosítás főbb állomásai és tevékenységei?

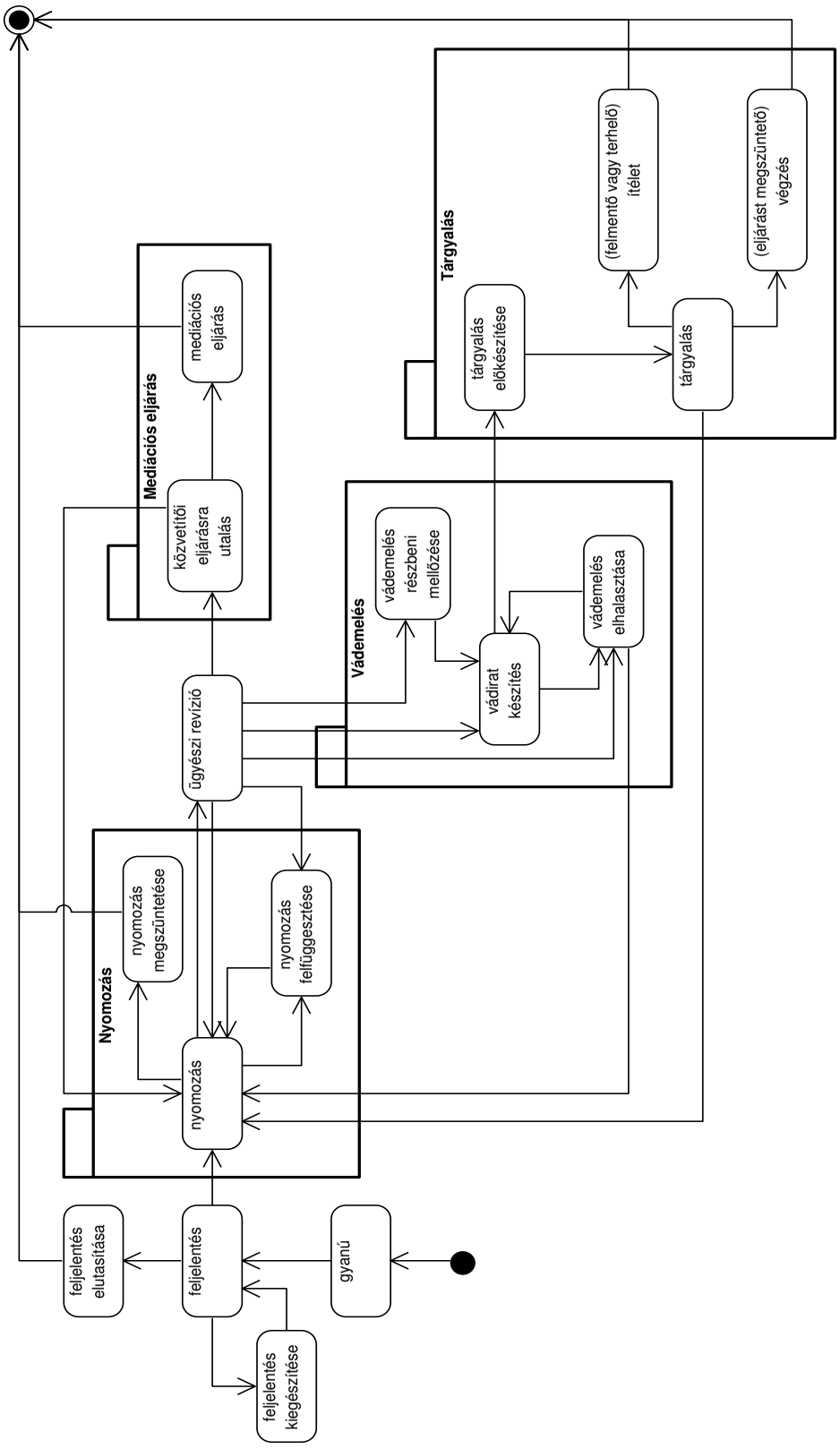
[86]

III.2.1 A büntetőeljárás

A büntetőeljárást a Be. szabályozza, ez alapján a főbb eljárási feladatok a

- nyomozás,
- vádemelés,
- mediációs eljárás,
- tárgyalás.

Ezek mellett természetesen a törvény több eljárási cselekményt is tartalmaz, amelyek összefoglalását a 27. ábra tartalmazza.



27. ábra – A büntetőeljárás főbb állomásai
(szerk.: Illési Zsolt)

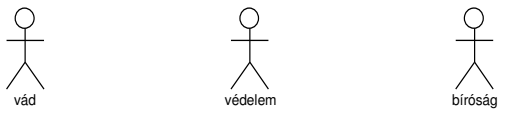
A modellben nem tüntettem fel az egyes állomások részleteit, ezek belső kapcsolatait. Ilyen almodelleket természetesen létre lehet hozni, ám az összkép felvázolásához és az egész eljárás modellezéséhez ezek a részletek feleslegesek, sőt zavaróak lennének.
Informatikai szakértői feladatokat jellemzően a büntetőeljárás 3 fő mozzanatában[166] végeznek, de a feljelentés, illetve a feljelentés kiegészítés során szintén előfordulhatnak szakértői feladatok főleg magánvádas ügyekben[167]. [41] [86]

Szakértői tevékenységekre elsősorban a nyomozati szakban kerül sor. Amennyiben a sértett szeretné a feljelentését megalapozni, ez úgy lehetséges, hogy a feljelentés előkészületei során saját szakembereivel vagy külső szakértő segítségével gyűjti össze és rendszerezi a bűncselekményre utaló nyomokat, hogy ezzel is segítse a nyomozás eredményességét. Mediációs eljárás vagy bírósági szakban is történik szakértői tevékenység, hiszen ilyenkor is felmerülhetnek újabb adatok, vagy régebbi tények kerülhetnek új megvilágításba, és ennek értelmezéséhez szükség lehet különleges szakértelemmel bíró személyek bevonására.

III.2.2 A büntetőeljárás szereplői

Miután sikerült modellezni, hogy milyen eljárás során mivel kell foglalkozni, felmerül annak a kérdése, hogy ki is végez informatikai szakértői feladatokat, illetve ki végezhet nyomfelkutatási, -biztosítási és -rögzítési tevékenységeket.

A modellezés kiindulópontjául először a klasszikus vád-védelem-bíróság triászából próbáltam kiindulni, de hamar be kellett látnom, hogy ebbe a hármas alapú modellbe a szakértő nem helyezhető el (ha másért nem, a Be.-ben meghatározott kizárások miatt).



28. ábra – A Be. szereplői (1): Általános modell ([45] alapján szerk.: Illési Zsolt)

[166] Nyomozás, mediációs eljárás és tárgyalás.

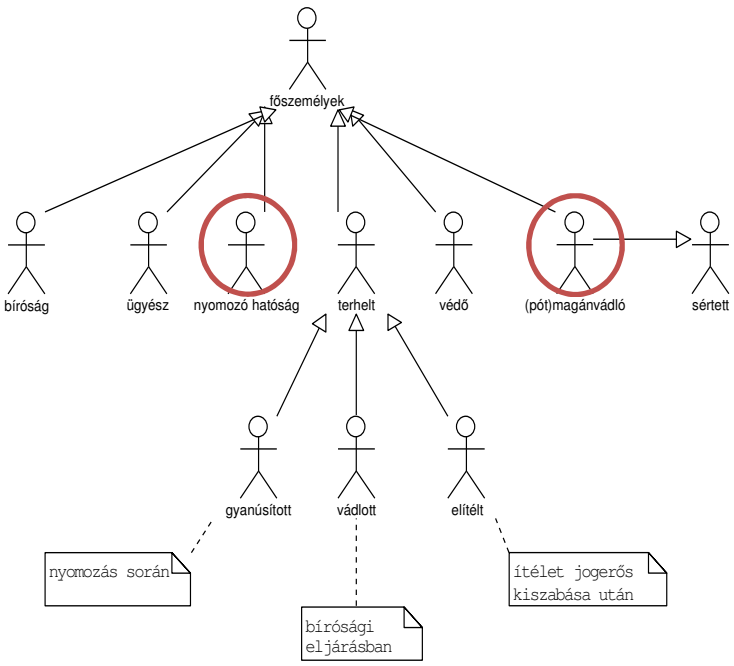
[167] Például interneten történő becsületsértés esetén.

A következő megközelítés alapja a Be.-ben betöltött szerep elsődlegessége, ez alapján a következő modell rajzolható fel:

29. ábra – A Be. szereplői (2): Szakértőket is tartalmazó modell ([45] alapján szerk.: Illési Zsolt)

Ez a modell a legfelső szinten ugyan közvetlenül még nem teszi lehetővé, hogy a szakértői feladatokat (is) ellátó szereplőket, azonban ennek a szereplői hierarchiának a kifejtése már lehetővé teszi a Be. szereplőinek katalogizálását (l. 30., 31. és 32 ábra).

Az egyes személyek kibontásával a fő személyekre a következő modell adódik:



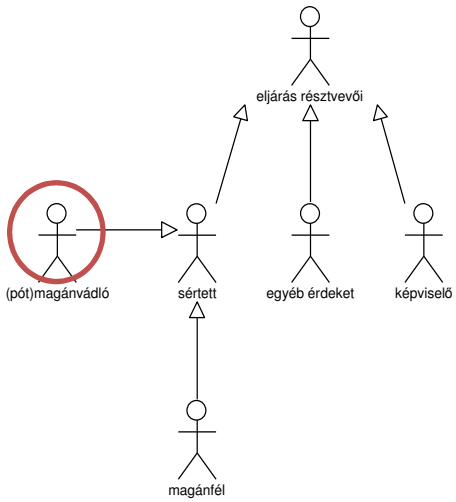
30. ábra – A Be. szereplői (3): Főszemélyek ([45] alapján szerk.: Illési Zsolt)

A főszemélyek funkcióinak vizsgálatával megállapítottam, hogy informatikai szakértői feladatokat a nyomozóhatóság és a pótmagánvádló szerepkört betöltő személyek játszhatnak.

A nyomozóhatóság sokszor végez szakértői jellegű tevékenységet. A nyombiztosítási, -felkutatási és -rögzítési tevékenység során megfelelően kell azonosítani és kezelni min-

den nyomhordozót – függetlenül attól, hogy fizikai vagy digitális nyom található-e rajta. A gyakorlatban ezen túl a hatóságok nyomelemzési és értékelési tevékenységeket is végeznek az információtechnológiai környezetből szerzett nyomok felhasználásával. Több nyomozati hatáskörrel rendelkező szerv – köztük például az NNI Csúcstechnológiai Bűnözés Elleni Osztálya – rendelkezik informatikai laborfelszereléssel, és ezeket aktívan használja is. A (pót)magánvádló szintén végezhet vagy végeztethet szakértői jellegű tevékenységeket. Mivel az általuk képviselt ügyek nem magánvádasak, ezért a (pót)magánvádlónak, amennyiben ezt a bíróság igazságügyi szakértő kirendelésével nem segíti, úgy saját eszközeire és szakértelmére hagyatkozva kell összegyűjtenie és prezentálnia az álláspontját megalapozó tényeket. Ez egy olyan esetben nyilvánvalóan informatikai szakkérdés, ha a sértettet például az interneten keresztül rágalmazták meg, és szükséges annak valószínűsítése, hogy ki lehetett az elkövető.

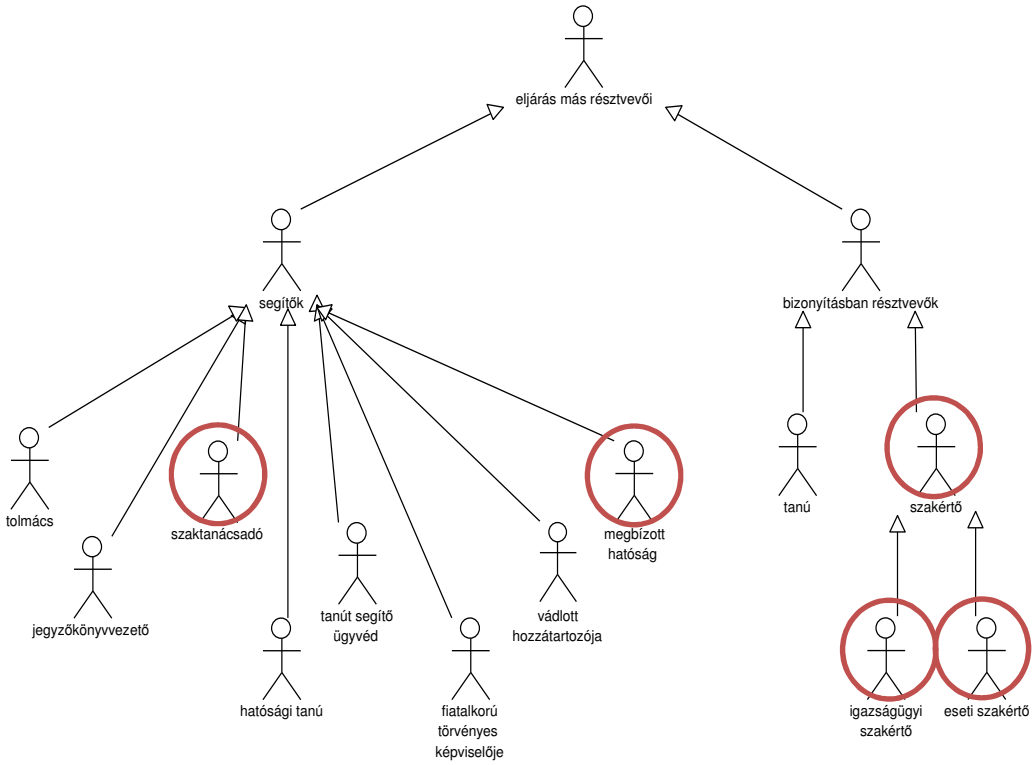
Az eljárás személyeinek elemzésével a következő modellt állítottam elő:



31. ábra – A Be. szereplői (4): Az eljárás résztvevői ([45] alapján szerk.: Illési Zsolt)

A Be. eljárás résztvevői közül speciális esetben csak a sértett (pótmagánvádlóként) – a sértetti szerepkörhöz tartozó speciális aktorként – végezhet az előző modellnél leírtak alapján szintén szakértői jellegű feladatokat.

Az eljárás más résztvevőinek funkcióelemzése során már több olyan szakértői tevékenységet betöltő személyt található, akiket szakértőként nevesít a Be.:



32. ábra – A Be. szereplői (5): Az eljárás más résztvevői ([45] alapján szerk.: Illési Zsolt)

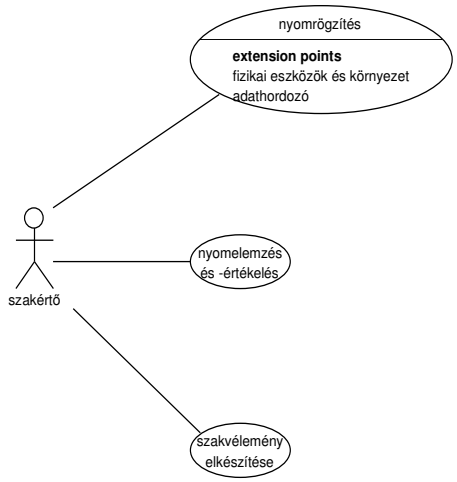
Ezek a szakértők az igazságügyi szakértő, az eseti szakértő és a szaktanácsadó. Ezek mellett informatikai szakértői tevékenységet láthat el a megbízott hatóság is, amennyiben információtechnológiai, hírközlési kérdésekben áll a bíróságok vagy a nyomozóhatóság rendelkezésére.

A résztvevőket azonosító modellek jól érzékeltetik, hogy nemcsak egy szakértői (vagy a szakértéssel összefüggő, szakértői jellegű) tevékenységet végző szerepkörű résztvevője van a büntetőeljárásnak, hanem több egymástól elkülönült személy vagy hatóság is végez ilyen feladatokat[168].

[168] Ezzel szemben csak az igazságügyi szakértőkkel szemben támaszt szakmai és egyéb szakmai jellegű garanciális feltételeket a hatályos jog; így nem követeli meg a többi szereplőtől a szakirányú végzettséget, szakmai gyakorlatot, nincs kötelező kamarai tagságuk sem, és nem, vagy csak részben köti őket a szakmai munkavégzés „kényszere”.

III.2.3 A szakértők feladatai

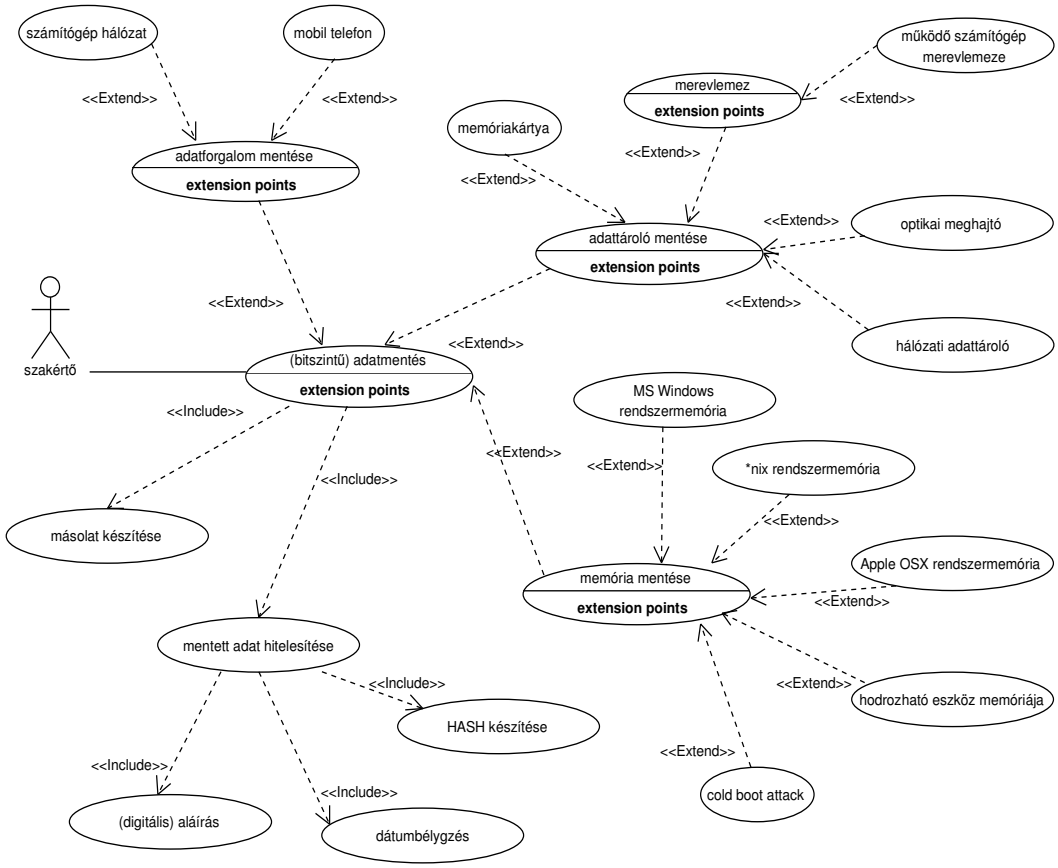
A Be. alapján felrajzolható az informatikai szakértés általános használati esetdiagramja is:



33. ábra – Informatikai szakértés általános feladatai (szerk.: Illési Zsolt)

A használati esetmodell kiegészítéseként meg kell jegyeznem, hogy a nyomrögzítés kapcsolódik a fizikai réteghez, a nyomelemzés és értékelés pedig együttesen a médiamenedzsment, a megjelenítési és az alkalmazási réteghez. A nyomelemzés és -értékelés sajnos olyan szerteágazó feladat, hogy ennek az elemzésére értekezésemben – többek között terjedelmi korlátok miatt – nem vállalkozom.

Az adatmaradványok rögzítésével kapcsolatos tevékenységek az absztrakt vizsgálati rétegmodell alapján a következők:



34. ábra – Digitális nyomrögzítés (adatmentés) **tevékenységei és kapcsolatuk (szerk.: Illési Zsolt)**

[86]

III.3 Helyszínhez (is) kapcsolódó nyomozási cselekmények

Kriminalisztikai szempontból *„helyszínen értjük azt a helyet, ahol a feltételezett bűncselekményt elkövették, avagy a bűncselekmény részét alkotó vagy azzal összefüggő egyéb részcselekmény, esemény stb. lezajlott”* [47 p. 174].

A fenti definíció alapján az információtechnológiai környezetben elkövetett bűncselekmények helyszíne – így a számítógép-hálózatot is magában foglaló helyszín – többes, sok lehetséges fizikai és virtuális helyszín együttesen alkothatja az elkövetés teljes színterét. Az információtechnológiai környezetben elkövetett bűncselekmény helyszíne ma-

gába foglalja az elkövetőt, a megtámadott számítógépét, a támadási útvonalba eső internetszolgáltatók kommunikációs eszközeit, valamint a támadás során használt számítógépeket, egyéb információtechnológiai eszközöket, valamint ezek logikai és fizikai környezetét.

A nyomozás során a helyszínhez a következő cselekmények kötődnek:

- **helyszíni szemle** – olyan nyomozási cselekmény, amely a Be. alapján folyik, és amely során a nyomozást végzők a meghatározott alakiságok (eljárási garanciák) mellett értékelik, rögzítik a helyszínen talált állapotot, helyzetet, körülményeket, és felkutatják a bűncselekménnyel kapcsolatos nyomokat és azok összefüggéseit;
- **bizonyítási kísérlet** – olyan vizsgálati cselekmény, mely során a nyomozást végzők azt vizsgálják, hogy egy esemény vagy jelenség meghatározott helyen és időben, módon, illetve körülmények között megtörténhetett-e;
- **helyszínelés** – speciális vizsgálati módszer, amely a helyszíni szemle és a kihallgatás sajátos kombinációjaként a terhelt vagy a tanú a bűncselekménnyel kapcsolatos helyet, cselekményt vagy tárgyi bizonyítási eszközt mutat meg;
- **felismerésre bemutatás** – olyan önálló nyomozási cselekmény, amely során sajátos körülmények mellett kell a tanúnak vagy a terheltnek személyt vagy tárgyat kiválasztania.

[44] [47] [86]

A fenti, helyszínhez kötött nyomozási cselekményeket a következő táblázat foglalja össze:

	Helyszíni szemle	**Bizonyítási kísérlet**	**Helyszínelés**	**Felismerésre bemutatás**
(Tipikusan) halasztathatatlan vagy megismételhetetlen?	mindkettő	egyik sem	egyik sem	csak megismételhetetlen
Helyszínhez vagy kihallgatáshoz kötött?	csak helyszínhez kötött	egyikhez sem kötött	mindkettőhöz kötött	csak kihallgatáshoz kötött
Helyettesíthetők-e az alanyok?	igen	igen	nem	nem
Tapasztalati jellegű vagy emlékezeti választású?	tapasztalati jellegű	tapasztalati jellegű (l. hallláspróba → ingerküszöb, hallhatóság)	emlékezeti választás	emlékezeti választás (l. beszédfelismerés, hangkiválasztás)

3. táblázat – A helyszíni szemle és a helyszínhez (is) kapcsolható nyomozási cselekmények elhatárolásának összefoglalása (forrás: [47 p. 204])

A nyomozási cselekmények lehetnek:

- attól függően, hogy a terheltnek és a környezetének tudomása lehet-e a vizsgálatokról
  - titkosak

  vagy
  - nyíltak;
- attól függően, hogy mennyire sürgős a végrehajtás lehetnek
  - halaszthatatlanok

  vagy
  - halaszthatóak.

A nyomozási tervtípusok a tárgyi vagy személyi vonatkozású gyanú és az indíték függvényében lehetnek:

- ismeretlen tetteses ügyek – bűncselekmény alapos gyanúja esetén;
- ismert tetteses ügyek – elkövetői alapos gyanú esetén;
- ismeretlen okú cselekményekkel kapcsolatosak – amikor bűncselekményre irányuló gyanú és esetleg elkövetői gyanú is fennáll, de a bűncselekményt megvalósító cselekménynek az oka ismeretlen.

[4] [47 pp. 251–253]

A nyomozás során gyűlnek össze azok a bizonyítékok, amelyek objektíven támasztják alá a terhelt bűnösségét vagy ártatlanságát. Ennek a folyamatnak lényeges lépése a szemle, ami egyrészt nyomozási cselekmény, másrészt bizonyítási eszköz, hiszen e cselekmény során a helyszínelők a büntetőeljárási kódex eljárási garanciái mellett észlelik és rögzítik a helyszínen talált állapotot, körülményeket, felkutatják a feltételezett bűncselekményekkel kapcsolatos nyomokat és azok összefüggéseit.

A szemle célja kettős:

- egyrészt olyan azonnal felhasználható információk nyújtása a nyomozás számára,
- másrészt bizonyítékok gyűjtése úgy, hogy a bizonyítékszerzés jogszerű legyen, megfeleljen a szakmai standardoknak[169], a tartalma pedig büntetőjogilag releváns (a perben felhasználható) legyen.

[47 p. 173]

A hatályos Be. szerint a bizonyítási eljárások a következők

- szemle,
- helyszíni kihallgatás,
- bizonyítási kísérlet,
- felismerésre bemutatás,
- szembesítés,
- szakértők párhuzamos meghallgatása.

[169] Megismételhetőség, tudományos-technikai megalapozottság.

A továbbiakban a szemle lépéseivel foglalkozom, mivel a helyszínhez kapcsolódó nyomozati cselekménynek a végrehajtása kritikus a jogszerű, szakszerű bizonyítékszerzés, ezáltal a hatékony és eredményes nyomozás szempontjából, valamint kiegészítem ezek szakirodalmi leírását olyan sajátos tevékenységekkel, amelyek túlmutatnak a tradicionális, csupán fizikai nyomhoz köthető feladatokhoz.

III.3.1 Helyszín felmérése

A kriminalisztika helyszín definíciója alapján (l. III.3 Helyszínhez (is) kapcsolódó nyomozási cselekmények fejezet) az információtechnológiai környezetben elkövetett bűncselekmények esetében a fenti definíció alapján rendkívül sok lehetséges fizikai és virtuális helyszín alkothatja az elkövetés teljes színterét. A helyszín magába foglalja a támadó számítógépét és annak környezetét, az érintett internetszolgáltatók kommunikációs eszközeit és azok környezetét, a támadás során felhasznált számítógépeket és azok környezetét, valamint a megtámadott információtechnológiai eszközt, rendszert, valamint annak környezetét.

A szemlére

- halaszthatatlan
- nyomozás elrendelését követően, nem halaszthatatlan

nyomozási cselekményként kerülhet sor.

A halaszthatatlan nyomozási cselekményként végrehajtott szemlék sajátossága a rövid felkészülés és a gyorsaság. Ennek ellenére a szemlét végrehajtónak ugyanolyan alapos munkát kell végeznie, mint nem halaszthatatlan esetben, mivel a felületesen, hiányosan végrehajtott szemle eredménytelen, nem nyújt elég információt a nyomozás folytatásához, nem biztosít elegendő releváns nyomot a bizonyításhoz.

A szemle eredményességének biztosítása érdekében a nyomozást végzőnek minden esetben fel kell készülnie, és gondoskodnia kell

- megfelelő számú és szakértelmű ember bevonásáról – például speciális hardver vagy szoftver ismeret biztosítása érdekében,
- a szükséges tárgyi, műszaki feltételek biztosításáról – például nyomkereső, nyomrögzítő műszerek, hardver és szoftver eszközök.

A személyi, tárgyi és műszaki feltételek biztosításának az alapja a hatékony felderítés. Előzetes információ hiányában előfordulhat, hogy bár egy jól képzett szakember megy ki a helyszínre, de az ott talált információtechnológiai rendszerhez nincs meg a szükséges kompetenciája, és amíg a megfelelő szakember kiérkezik, addig lényeges adatok vesznek el.

A gyors, hatékony szemlének feltétele a nyombiztosítási, nyomfelkutatási és nyomrögzítési módszerek, a dokumentálás (például nyomtatványok) szabványosítása.

A helyszín felmérésekor lényeges annak megállapítása, hogy a helyszín:

- **valódi** – egy megtörtént bűncselekmény tényleges helyszíne,
- **koholt** (beállított) – egy meg nem történt bűncselekmény „imitációja”,
- **megváltoztatott**, vagy **részlegesen beállított** – egy valós bűncselekmény végrehajtását részben másnak feltüntetett, más elkövetőre vagy más elkövetési módszerre utalóvá alakított,
- **többes** (tagolt) – az elkövető, a felhasznált eszközök és a célpont földrajzilag is szétt agoltan találhatók meg[170],
- **mozgó** – valamilyen közlekedési eszköz felhasználásával végrehajtott bűncselekmény esetén (például wardriwing), vagy
- **élő** – működő információtechnológiai rendszerrel kapcsolatos.

A szemlével rokon cselekmény a házkutatás, ami ház, lakás, egyéb helyiség, vagy azokhoz tartozó bekerített hely, továbbá az ott elhelyezett jármű átkutatását, illetőleg számítástechnikai rendszer vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozó átvizsgálását jelenti az eljárás eredményessége érdekében.

Házkutatást alapos gyanú alapján a bíróság, az ügyész, illetőleg, ha az ügyész másképp nem rendelkezik, a nyomozó hatóság rendelhet el zárt helyiséggel rendelkező személy akarata ellenére. Azonban ha a zárt helyiség felett rendelkező természetes vagy jogi személy[171] kéri vagy beleegyezik, úgy házkutatás helyett szemlét lehet tartani.

[170] Ez a helyszín típus különösen jellemző az információtechnológiai környezetben elkövetett bűncselekményekre.

[171] A sértett, terhelt, érintett, például ISP.

A szemle során lehetőség van arra, hogy dolgokat[172], számítástechnikai rendszereket, az ilyen rendszerrel rögzített adatokat a hatóság lefoglaljon, ha azok

- bizonyítási eszközök

vagy

- a törvény értelmében elkobzandók[173]

vagy

- amelyre vagyonelkobzás rendelhető el.

[4] [44] [47 pp. 174–176]

Esetenként a nyomozó hatóság nem foglalja le az potenciális nyomhordozókat, például ha a lefoglalás miatti rendszerkiesés aránytalan érdeksérelemmel járna, hanem a helyszínen elemzi az ott található információtechnológiai eszközöket, menti le azok adattartalmát. A nyomelemzés során felmerülhetnek olyan nyomok, bizonyítékok, amelyek további bizonyítékok meglétét valószínűsíthetik, és újra indulhat a helyszíni felmérés és a kapcsolódó cselekménysorozat.

III.3.2 Helyszínbiztosítás

A helyszín biztosítása során a cél a változtatások, változások megakadályozása. A helyszín biztosítása történhet passzív vagy aktív módon. A passzív helyszínbiztosítás során a helyszínelők nem módosítják a helyszínt, csak a helyszín körülhatárolásáról, esetleg élőerős védelméről gondoskodnak. Aktív helyszínbiztosítás során a helyszínelők a nyomok megőrzése érdekében olyan intézkedéseket hajtanak végre, amelyek, bár részben módosítják a helyszínt, de gondoskodnak a releváns nyomok megőrzéséről[174].

A helyszínelőnek a biztosítás során gyorsan kell felmérnie, hogy hol vannak a helyszín valódi határai, hol lehetnek olyan érintett számítástechnikai eszközök, amelyek vezetékes vagy vezeték nélküli kapcsolattal csatlakoznak a szűk értelemben vett helyszínen lévő számítógéppel. Informatikai igazságügyi szakértők anekdotáznak arról, hogy a feltételezett helyszínt az elkövető internetes kamerával figyelte, és valamilyen távoli kapcso-

[172] Adathordozókat, számítógépet vagy egyéb eszközöket.

[173] Például pedofil képek, egy számviteli fegyelem megsértését bizonyító könyvelési rendszer adatbázisa, vagy egy hamis tanúzással kapcsolatos üzenetváltást tartalmazó e-mail levelezés.

[174] Külső helyszínen letakarással védik a nyomokat, információtechnológiai környezetben elkövetett bűncselekmények esetén leválasztják a hálózatról a helyszínen lévő számítógépeket.

laton keresztül menedzselte – pontosabban szisztematikusan megsemmisítette – az érintett információtechnológiai rendszert és annak adatait. A fentiek figyelembevételével a virtuális helyszín biztosításáról – a fizikai helyszínéhez hasonlóan – kell gondoskodni, de komolyan mérlegelendő, hogy mely eszközök tartalma vizsgálható kikapcsolt állapotban, és melyek adatait kell/lehet az élő információtechnológiai környezetben vizsgálni.
[4] [44] [47 p. 177]

III.3.3 Helyszíni szemle lefolytatása

A helyszíni szemle alapvetően egy statikus (összképrögzítő) és egy dinamikus (nyomkereső) szakaszra osztható.

A statikus szakaszban a helyszínelő célja az összkép megfigyelése, az ott lévő valamennyi jelenség és körülmény rögzítése anélkül, hogy a helyszínen lévő tárgyakat elmozdítaná, vagy beavatkozna az ott lezajló jelenségekbe. Célja az elkövetés feltételezett központjának, eszközeinek az azonosítása, illetve információszerzés az elkövetés módjáról. Egy számítógépes munkahely, amely mellett szitázott, de nyers DVD-k sorjáznak, már „ránézésre" is kellő támpontot nyújt egy szerzői jogsértés vizsgálatához.

A statikus szakaszban kell arról dönteni, hogy a „fizikai" vagy a „digitális" nyomok felkutatása, rögzítése legyen az elsődleges feladat. Amennyiben az előzetes puhatolás valószínűsíti az információtechnológiai környezetben elkövetett bűncselekmény elkövetését – és a gyanú szerint az adatok lényeges elemét szolgáltatják majd a bizonyítási eljárásnak –, úgy célszerű először az adatok konzerválására fókuszálni, de ebben az esetben különös figyelmet kell fordítani arra, hogy az információtechnológiai szakértő a lehető legkevesebb fizikai nyomot (például ujjlenyomat) tegyen tönkre. A statikus szakasz dokumentálási eszköze elsősorban a fényképezőgép, videó, diktafon.

A dinamikus szakaszban történik a nyomok szisztematikus keresése, ami kiterjed a helyszínen lévő valamennyi objektumra, eszközre. A helyszínelők célja ebben a szakaszban az, hogy valamennyi releváns nyom felderítésre és rögzítésre kerüljön, ami bizonyítékul szolgálhat, vagy támpontot nyújt a későbbi nyomozati cselekményekhez, és információt szolgáltat az elkövetés idejéről, módjáról, esetleg az elkövető személyéről.

Előfordulhat, hogy a helyszíneléssel egyidejűleg az elkövető még a virtuális helyszínen aktív, és a hálózaton keresztül tevékenykedik a vizsgált fizikai vagy logikai helyszínhez kapcsolódó számítógépen. Az is lehetséges, hogy a vizsgált információtechnoló-

giai környezetben fut olyan program, ami az ügy szempontjából releváns adatokat tartalmaz, ami csak a futtató eszköz memóriájában található meg (például hálózati kapcsolódási adatok, kriptográfiai kulcsok). A szemle lefolytatása során az informatikai ügyekkel foglalkozó szakembereknek különösen nagy gonddal kell eljárniuk, hiszen a számítógépek kikapcsolásával esetleg releváns adatok[175] veszhetnek el, a számítógépek izolációja a gép önrombolását, az adattartalom törlését, titkosítását idézheti elő.

A szemle lényeges, de el nem hanyagolható feladata a nyomoknak a rögzítése – adatok esetén például digitális aláírással hitelesített, de legalább hash lenyomattal ellátott másolat készítésével.

A nyomrögzítés során készül el a bűnjeljegyzék, ami az információtechnológiai eszközök és adathordozók egyedi azonosítását és leltározását jelenti. A bűnjeljegyzékbe az egyes számítógépeket fel lehet venni egységként[176], de ebben az esetben gondoskodni kell a számítógép szétszerelésének detektálhatóságáról, például plomba vagy lepecsételt ragasztószalag alkalmazásával.

[4] [44] [47 pp. 178–181]

III.3.4 Egységesített fizikai és digitális kriminalisztikai tevékenységmodell

A helyszín felmérése, a helyszínbiztosítás és a helyszíni szemle leírásakor a következő elemi tevékenységek kerültek megemlítésre:

- felkészülés, helyzetértékelés;
- nyomfelkutatás;
- helyszín biztosítása:
  - fizikai nyombiztosítás,
  - hálózati adatok rögzítése;
- nyomrögzítés:
  - fizikai nyomok rögzítése,
  - adatmentés;
- nyomelemzés.

[175] Kapcsolati információk, jelszavak, titkosítási kulcsok.

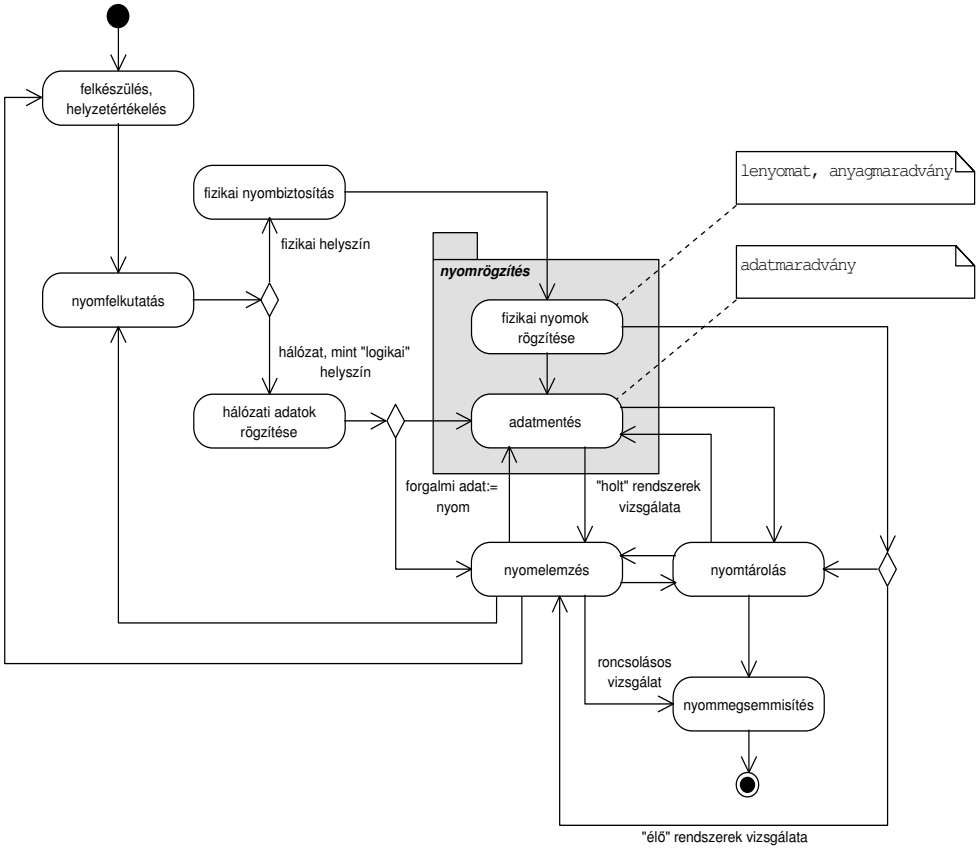
[176] A számítógépet és valamennyi beépített alkatrészét együttesen.

A nyomfelkutatás, -rögzítés, -biztosítás teljes körű modellezéséhez figyelembe kell venni a nem közvetlen nyomozati tevékenységként megjelenő

- nyomtárolási és
- nyom-megsemmisítési

tevékenységeket is.

Az azonosított tevékenységi elemek és az egyes helyszínhez is kapcsolódó nyomozati cselekmények leírása alapján felrajzolható a fizikai és információtechnológiai nyomfelkutatás, -rögzítés, -biztosítás egyesített modellje. Ezt a modellt a 35. ábra foglalja össze:



35. ábra – Egyesített fizikai és digitális nyomfelkutatási, -rögzítési, -biztosítási és nyomelemzési tevékenységmodell (szerk.: Illési Zsolt)

[86]

Következtetések

Az információtechnológiai elemet is magában foglaló nyomfelkutatási, -rögzítési, -biztosítási és nyomelemzési események összetett tevékenységet jelentenek. Az ilyen feladat elvégzése során a szakértői szerepet betöltő résztvevőknek egységes szerkezetben kell elvégeznie a fizikai és a digitális nyomokkal kapcsolatos teendőket mind a valós, mind a virtuális helyszínen úgy, hogy a lenyomat, anyagmaradvány és az adatmaradvány egymást kiegészítve segítse a későbbi büntetőeljárást, csökkentse a büntetőügyekre oly jellemző bizonyítékínséget, növelje a felderítés eredményességét és hatékonyságát.

Ez a tevékenység nagyon összetett és komoly felkészülést igényel. Az értekezésemben áttekintettem azokat a legfontosabb kérdéseket, amelyek szükségesek egy egyesített fizikai és digitális nyomfelkutatási, -rögzítési, -biztosítási és nyomelemzési tevékenység protokoll kidolgozásához, illetve a vizsgálatokat leíró igazságügyi szakértői módszertani levél elkészítéséhez. Összefoglaltam a digitális helyszínelés főbb feladatait, a felkészülés és végrehajtás során végrehajtandó résztevékenységeket, illetve azonosítottam a sikerkritériumokat. A fejezetben megalkotott modellek bizonyítják, hogy az eljárási protokollok és szakmai módszertani levelek különböző pontjai egységes modellbe integrálhatók.

A jogszabályok alapján meghatároztam az információtechnológiai környezethez kapcsolódó krimináltechnikai tevékenységekkel kapcsolatos szakmai elvárásokat.

A hatályos büntetőeljárási törvény alapján elkészítettem a büntetőeljárás főbb állomásait, azok csoportosítását és kapcsolatait tartalmazó állapotmodellt. A modellezéssel egyidejűleg meghatároztam azokat a tevékenységcsoportokat, ahol szakértői feladatok végrehajtódnak, és megállapítottam, hogy szakértői feladatokat jellemzően a büntetőeljárás három fő mozzanatában végeznek.

A szakirodalmi elemzés és a saját tapasztalataim alapján elkészítettem a büntetőeljárásban szakértői feladatokat ellátó szereplők modelljeit. Megállapítottam, hogy a klasszikus vád-védelem-bíróság hármasára épülő modell alkalmatlan a szerepek egyértelmű azonosítására és az aktorok (szereplők) tevékenységeinek függőségeinek (általános-speciális kapcsolatainak) feltárására. Ezt csak a Be.-ben betöltött főszemély és az eljárás más résztvevőinek megközelítése alapján lehet meghatározni. Elkészítettem a szerep modelleket, amelyek kibontása alapján valamennyi főbb – információtechnológiai feladatokat végző, ilyen kérdésekben szakkérdéseket megválaszoló vagy tanácsadó – szakértő szerepkörrel is rendelkező személyt azonosítottam. A szakértői feladatokat ellátó aktorokhoz

elkészítettem az általános használati esetmodellt. Az általános modell és az értekezésemben korábban ismertetetett vizsgálati rétegmodell kombinációjaként meghatároztam a szakértők részletes tevékenységeit és azok kapcsolatát definiáló részletes esetmodellt.

A helyszínhez (is) kapcsolódó nyomozási cselekmények áttekintésekor az általános helyszín felmérési, biztosítási, valamint a helyszíni szemle lefolytatási tevékenységek leírását kiegészítettem az információtechnológiai vizsgálatokhoz kapcsolódó szempontokkal, amelyek összhangban vannak az értekezésem első fejezetében leírt digitális nyom fogalmával, a digitális nyomok rendszertanával. A fejezetben ismertettem végül egy olyan egyesített fizikai és digitális nyomfelkutatás, -rögzítési, -biztosítási és nyomelemzési tevékenységmodellt, ami minden olyan tevékenységet és ezek kapcsolatát tartalmazza, ami a fizikai és virtuális helyszínnel is rendelkező helyszínhez (is) kötődő tevékenységet takar.

A fejezetben ismertetett modellek, kiegészítve az értekezésem korábbi fejezeteiben ismertetett egyéb modellekkel, így különösen a(z)

- 3. ábra – A bűncselekmények állapotdiagramja
- 4. ábra – Büntetőjogilag releváns tények osztálydiagramja
- 5. ábra – Nyomok általános állapotdiagramja

egységes alapot szolgáltatnak a helyszínhez (is) köthető hatósági eljárási protokollok és az informatikai igazságügyi szakértői módszertani levelek elkészítéséhez. A szabványos modellezési technika továbbá lehetővé teszi a modellek alapján történő alkalmazásfejlesztést, így mind a hatósági, mind az igazságügyi szakértői munka szoftveres támogatását.

Véleményem szerint az általam megalkotott modellek és feltárt relációk nemcsak az információtechnológiai kapcsolódású feladatokhoz, hanem egyéb általános kriminál-technikai vizsgálatokhoz és kapcsolódó hatósági protokollok megalkotásához nyújtanak alapot.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Az infokommunikáció egyre jobban áthatja a mindennapjainkat, beépül a társadalmi-gazdasági folyamatokba. A technológia penetrációjával azonban megnőtt az egyének, szervezetek, államok függősége, ezen keresztül a sebezhetősége. Ennek az egyik sajátos megjelenési formája új típusú konfliktusok, az információtechnológiai környezetben elkövetett támadások és bűncselekmények megjelenése. E konfliktusok békeidőben a bíróságokon dőlhetnek el. A bírósági jogérvényesítés a jog talaján áll, azonban a hatékony és eredményes jogérvényesítéshez kellő mennyiségű és minőségű bizonyítékra van szükség. Új típusú bizonyítékforrásként – az új típusú technológia talaján – megjelent informatikai védelem egyik speciális alága, amelynek fókuszában **az informatikai rendszerekben keletkező nyomok és ezek elemzése** áll. Ez egy olyan **interdiszciplináris terület**, amely **a jog, a kriminalisztika és az informatika metszetében** található: az informatikai igazságügyi szakértés.

A jelenlegi nyomozási tevékenységek, informatikai igazságügyi módszerek azonban nem alkotnak összefüggő rendszert. A jogszabályok eltérő módon és mértékben határozzák meg a szakértői szerepben eljárókkal szemben megkövetelt szakmai kompetencia szintjét. A forenzikus vizsgálatok jelenleg operációs rendszer-, fájlrendszer-, számítógép-hálózat-, mobiltelefónia-specifikus, azaz szigetszerű megoldásból állnak, amelyek ugyan egyenként megállják a helyüket, kiállják a tárgyalóterem próbáját, de nem alkotnak koherens szakmai módszertant.

Az értekezésemben **áttekintettem** a jog és a kriminalisztika nyomokkal, bizonyítékokkal és bizonyítással foglalkozó rendszerét, és **megállapítottam, hogy a nyom fogalma szolgál kiindulási alapul** a bűnügyi nyomozás során végrehajtott nyombiztosítási, -felkutatási, -rögzítési tevékenységnek, illetve a krimináltechnikai vizsgálatok során elvégzett tevékenységnek. A fizikai nyom és az információtechnológiai környezetben fellelhető nyomként értelmezhető adatnyomok összevetésével **megállapítottam**, hogy a **lenyomat és anyagmaradvány sajátosságaira alapozó nyom fogalma nem adekvát, nem fejezi ki megfelelően a digitális nyomképző, nyomhordozó és nyomképződési folyamat jellegzetességeit**. Ezért **megalkottam egy olyan nyomfogalmat** (digitális nyom), amely összhangban van mind a traszológiai, mind a kriminalisztikai nyom fogalmával, és **megfelel az információtechnológiai környezet karakterének**. **A digitális**

nyom fogalmi rendszerének tisztázását követően osztályoztam, és az egyedi jellemzők alapján rendszereztem a digitális nyomokat.

Értekezésemben az általános kriminalisztikai jellemzők mellett **feltártam az információtechnológia egyedi jellegzetességeit is, illetve bemutattam ezeknek a sajátosságoknak a krimináltechnikai vizsgálatokra gyakorolt következményeit** is.

A digitális nyom taxonómia elkészítését követően rendszereztem az ezekkel kapcsolatos tevékenységeket. A rendszerezés alapproblémája korábban az volt, hogy miképp lehet a sokrétű informatikai igazságügyi szakértői tevékenységeket úgy osztályozni, hogy az így kapott tevékenység-csoportok zárt logikai egységet alkossanak, lehetőleg ne ismétlődjenek az egyes csoportokba sorolt tevékenységek, továbbá valamilyen szinten definiálják a feladat elvégzéséhez szükséges kompetenciákat. A feladat kidolgozásában segítségül hívtam Brian Carrier absztrakt réteg-megközelítési modelljét. Ezt az **alapmodellt továbbfejlesztettem**, kiegészítettem azokkal a szükséges elemekkel, amelyek lehetővé tették azt, hogy már komplex módon alkalmas legyen az információtechnológiai környezetben fellelhető digitális nyomok krimináltechnikai vizsgálataira, a vizsgálatok során elvégzett résztevékenységeknek, az alkalmazott hardver és szoftver eszközöknek, valamint a feladatvégzéshez szükséges szakmai kompetenciáknak a rendszerezésére.

Miután meghatároztam a digitális nyom fogalmát, meghatároztam a nyomok taxonómiáját, és rendszerbe foglaltam a kapcsolódó krimináltechnikai tevékenységeket, majd meghatároztam a vonatkozó módszertani levelekkel kapcsolatos jogszabályi követelményeket, **elkészítettem büntetőeljárás szakértéssel kapcsolatos magas szintű, áttekintő modelljét**. A tevékenységek, a szereplők meghatározása után, a nyom életciklus modelljének figyelembevételével kiegészítettem a hagyományos nyombiztosítási, -felkutatási és -rögzítési modellt, hogy az tartalmazzon minden az információtechnológiai környezetben fellelhető digitális nyomokkal kapcsolatos releváns részletet. **Ennek a feladatnak az összegzéseként elkészítettem egy egységes UML modellrendszert, amely integrálja a fizikai és az információtechnológiai sajátosságokat magában foglaló eljárásokkal kapcsolatos főbb kriminalisztikai kérdéseket.** Az általam készített modellrendszer nemcsak elemzés, hanem véleményem szerint megfelelő alapot szolgáltat a vonatkozó kriminalisztikai protokoll, továbbá igazságügyi szakértői levelek elkészítéséhez.

Véleményem szerint kutatásaim eredményesek voltak, a kitűzött tudományos célkitűzéseimet elértem. Az értekezésemben összefoglaltakat a további informatikai igazságügyi szakértői tevékenységeim során sikerrel tudom majd hasznosítani. Úgy vélem, hogy az

eredményeim nemcsak nekem vagy egy szűk szakértői kör számára hasznosak, hanem szélesebb körben, így a védelmi és a civil szféra számára is nyújtanak hasznosítható eredményeket.

ÚJ TUDOMÁNYOS EREDMÉNYEK

Az elvégzett kutatómunkám alapján új tudományos eredménynek tekintem az alábbiakat:

1) **Meghatároztam a digitális nyom fogalmát, összhangban a kriminalisztikai és traszológiai** fizikai nyom (anyagmaradvány és lenyomat) **fogalmával**.

2) **Osztályoztam és az egyedi jellemzők alapján rendszereztem a digitális nyomokat.**

3) Brian Carrier **absztrakt réteg-megközelítési modelljé**nek **továbbfejlesztésével és kiegészítésével, egy olyan komplex taxonómiára tettem javaslatot, ami alkalmas valamennyi információtechnológiai vizsgálat rendszerezésére és leírására**, továbbá a szükséges kompetenciák megállapítására.

4) **Kidolgoztam egy magas szintű UML modellrendszert, amely integrálja a fizikai és az információtechnológiai sajátosságokat magában foglaló eljárásokkal kapcsolatos főbb kriminalisztikai kérdéseket**. Az általam kidolgozott modellrendszer megalapozza a vonatkozó szakmai protokollok és informatikai igazságügyi szakértői módszertani levelek elkészítését.

AJÁNLÁSOK

Az értekezésemben leírtakat javaslom felhasználni a felsőoktatásban a krimináltechnikai és kriminalisztikai tárgyak keretében, továbbá az igazságügyi szakértők informatikai szakmai továbbképzésében.

Az értekezésemben definiált krimináltechnikai vizsgálatok rétegmodellje alkalmas az információtechnológiai krimináltechnika kutatásai osztályozására, az egyes módszerek és technikák kapcsolatrendszerének feltárásra, rendszerezésére.

Az általam javasolt magas szintű nyomfelkutatási, -biztosítási és -rögzítési modellt felhasználását javaslom a védelmi szféránál, különösen annak nyomozati tevékenységet folytató szervezeteinél.

Az értekezésem kiindulópontja lehet az igazságügyi szakértők informatikával kapcsolatos módszertani leveleinek.

Dunaújváros, 2012. szeptember 30.

Illési Zsolt

A TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓIM

Lektorált folyóiratban megjelent cikkek

1) **KOVÁCS László, ILLÉSI Zsolt**: Cyberhadviselés
in Hadtudomány XXI. évfolyam 1–2. szám, pp. 29–41
ZMNE, Budapest, 2011. május
ISSN 1215–4121

2) **ILLÉSI Zsolt**: Az igazságügyi szakértés modellezése
in Hadmérnök, V. évfolyam 4. szám, pp. 122–132
ZMNE, Budapest, 2010.
ISSN 1788–1919

3) **ILLÉSI Zsolt**: WiFi hálózatok igazságügyi szakértői elemzése:
WiFi hálózatok felderítése
in Hadmérnök IV. évfolyam, 3. szám, pp. 285–302
ZMNE, Budapest, 2009. szeptember
ISSN 1788–1919

4) **ILLÉSI Zsolt**: Kriminálmtechnika szerepe az informatikai védelem területén
in Hadmérnök IV. évfolyam, 1. szám, pp. 170–183
ZMNE, Budapest, 2009. március
ISSN 1788–1919

5) **ILLÉSI Zsolt**: Számítógép-hálózatok kriminálmtechnikai vizsgálata
in Hadmérnök, IV. évfolyam, 4. szám, pp. 163–175
ZMNE, Budapest, 2009. december
ISSN 1788–1919

6) **ILLÉSI Zsolt**: Open source IT forensics – avagy nyílt forráskódú programok felhasználása az informatikai igazságügyi szakértésben
in Bolyai Szemle, XVII. évfolyam, 4. szám, pp. 181–195
ZMNE, Budapest, 2008.
ISSN: 1416–1443

7) **ILLÉSI Zsolt**: Botnetek kialakulása, használatuk, trendjeik
in Hadmérnök. III. évfolyam, 2. szám, pp. 129–137
ZMNE, Budapest, 2008. június
ISSN 1788–1919

8) **ILLÉSI Zsolt**: Számítógép-hálózat audit
Networkshop 2008. [Online]
Nemzeti Információs Infrastruktúra Fejlesztési Intézet, 2008. március
http://nws.niif.hu/ncd2008/docs/phu/084.pdf
[utolsó megtekintés: 2012.09.30.]

Idegen nyelvű kiadványban megjelent cikkek

1) **ILLÉSI Zsolt**: NEEDLE IN A HAYSTACK – A Quest to Identify, Classify, and Reduce Data to Find Adequate Digital Evidence
in VIII Konferencija Naukova Studentóv 8th Students konference, pp. 275–281
Oficína Wydawnicza Politechniki Wroclawskiej, Wroclaw, Poland, 2010.
ISSN 1732–0240

Konferencia kiadványban megjelent előadás

1) **ILLÉSI Zsolt**: Information violation (?) and computer forensics
Óbudai Egyetem, Budapest: 2011.11.19.
ISBN 978–615–5018–20–6

2) **ILLÉSI Zsolt**: Bizonyítás a kibertérben
Hacktivity 2011. [Online]
https://hacktivity.com/hu/archivum/videostream/139/hu/
[utolsó megtekintés: 2012.09.30.]

3) **ILLÉSI Zsolt:** Tűt a szénakazalban
Hacktivity, [Online], 2010.
https://hacktivity.com/hu/letoltesek/archivum/47/
[utolsó megtekintés: 2012.09.30.]

4) **ILLÉSI Zsolt**: Computer forensics need for a domestic and/or EU ‘hash factory’
in XX VI. Nemzetközi Kandó Konferencia kiadványa
Óbudai Egyetem, Budapest, 2010.11.04.
ISBN 978–963–7158–04–9

5) **ILLÉSI Zsolt**: Hackers beware! – Digitális nyomok az informatikai rendszerekben
Hacktivity 2009, [Online], 2009.
https://hacktivity.com/hu/letoltesek/archivum/105/
[utolsó megtekintés: 2012.09.30.]

6) **ILLÉSI Zsolt**: Rádiós hálózatok kriminál technikai vizsgálata
in 2009. XXV. Nemzetközi Kandó Konferencia kiadványa
Óbudai Egyetem, Budapest, 2009.
ISBN 978–963–7158–04–9

FELHASZNÁLT IRODALOM

1) **MUNK Sándor**: Információbiztonság vs. informatikai biztonság
in Hadmérnök (Robothadviselés 2007. különszám) [Online]
ZMNE, Budapest, 2007.11.27.
http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/munk_rw7.html
ISSN 1788–1919
[utolsó megtekintés: 2012.09.30.]

2) **VASVÁRI György**: Bankbiztonság
Műegyetemi kiadó, **BUDAPEST**, 1995.
ISBN: 963–8545–37–2

3) **TOUCHE Ross & Co.**: Computer **CONTROL** and Audit
Institute of Internal Auditors, Altaminte Springs, USA, 1978.
n.a.

4) **ILLÉSI Zsolt**: Krimáltechnika szerepe az informatikai védelem területén
in Hadmérnök IV. évfolyam, 1. szám, pp. 170–183
ZMNE, Budapest, 2009. március,
ISSN 1788–1919

5) **IT café**: Túl sokáig ül a rendőrség a lefoglalt számítógépeken
IT café, [Online], 03 04 2009
http://itcafe.hu/hir/sokaig_ul_a_rendorseg_a_lefoglalt_szamitogepeken.html
[utolsó megtekintés: 2012.09.30.]

6) **FÖLDVÁRI József**: Magyar Büntetőjog Általános rész, 4., átdolgozott kiadás
Osiris Kiadó, Budapest, 1998.
ISBN 963 379 496 X

7) **ÁDÁNY Tamás Vince, BARTHA Orsolya, TÖRŐ Csaba** (szerk.): A fegyveres összetűzések joga
Zrínyi Kiadó, Budapest, 2009.
ISBN 978–963–7060–59–5

8) **BOLGÁR Judit, SZTERNÁK Nóra, SZTERNÁK György**: A terrorizmussal kapcsolatos kutatás legújabb eredményei.
Hadtudományi Doktori Iskola, [Online], 2005.
http://www.zmne.hu/dokisk/hadtud/bolgar.pdf
ISSN 1788–1919
[utolsó megtekintés: 2012.09.30.]

9) **Andrew M. COLARIK**: Cyber Terrorism: Political and Economic Implications
Idea Group Publishing, USA: 2006.
ISBN 1–59904–021–2

10) **HAIG Zsolt**: Internet terrorizmus
Hadtudományi Doktori Iskola, [Online], 2006.
http://www.zmne.hu/dokisk/hadtud/terror/lekt_Haig_Zsolt.pdf
ISSN 1788–1919
[utolsó megtekintés: 2012.09.30.]

11) **ZETTNER Tamás**: Fél nap alatt 12 millió dollárt zsebelt be a bűnbanda
IT café, [Online], 2009.11.11.
http://itcafe.hu/hir/fel_nap_alatt_12_millio_dollar_csalas.html
[utolsó megtekintés: 2012.09.30.]

12) **MUHA Lajos**: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme című doktori (PhD) értekezés
ZMNE, Budapest, 2007.

13) **KOVÁCS László, HAIG Zsolt**: Kritikus információs infrastruktúrák elleni fenyegetések, Kritikus információs infrastruktúrák védelme
in Szenes Katalin (szerk.): Az informatikai biztonság kézikönyve. 30. Aktualizálás, pp. 137–170.
Verlag Dashöfer Szakkiadó, Budapest: 2008.
ISBN 963 9313 12 2

14) **KOVÁCS László**: Az információs terrorizmus elleni tevékenység kormányzati feladatai
in Hadmérnök. 2008, Vol. 2., pp. 138–148
ISSN 1788–1919

15) **KOVÁCS László**: Lehetséges-e terrortámadások végrehajtása
az információs rendszereken keresztül?
Nemzetvédelmi egyetemi közlemények: a ZMNE tudományos lapja, 10. évfolyam 3. (tematikus) szám 2006. [Online], 2006.07.01.
http://www.zmne.hu/dokisk/hadtud/Kovacs2.pdf
ISSN 1788–1919
[utolsó megtekintés: 2012.09.30.]

16) **Bradley GRAHAM**: Hackers Attack Via Chinese Web Sites
The Washington Post, [Online], 2005. 08. 25.
http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html
[utolsó megtekintés: 2012.09.30.]

17) **SZEGEDINÉ Lengyel Piroska**: Számítógépes bűnözés avagy fiatalok a cyber-térben
in Hadmérnök, pp. 367–379
ZMNE, Budapest, 2010.06.
http://hadmernok.hu/2010_2_szegedine1.pdf
ISSN 1788–1919
[utolsó megtekintés: 2012.09.30.]

18) **Bert-Jaap KOOPS**: Crypto Law Survey
[Online], 2010.
http://rechten.uvt.nl/koops/cryptolaw/
[utolsó megtekintés: 2012.09.30.]

19) **P. SOMMER**: Challenges today in large computer crime task forces
in Digital Investigation, Vol. Vol. 1 No. 1.
Elsevier Ltd., USA, 2004.
ISSN 1742–2876

20) **HAIG Zsolt**: Az információs társadalmat fenyegető információ alapú veszélyforrások
in Hadtudomány, 2007, XVII. évfolyam, 3. szám.
Magyar Hadtudományi Társaság, Budapest
ISSN 1215–4121

21) **ZETTNER Tamás**: Amikor az életed a tét
IT café, [Online], 2009.11.09.
http://itcafe.hu/hir/amikor_az_eleted_a_tet.html
[utolsó megtekintés: 2012.09.30.]

22) **DAJKÓ Pál**: Kínos baki: közel százezer vétlen weboldalt tiltottak le a netről
IT café, [Online], 2011.02.17.
http://itcafe.hu/hir/dhs_ice_homeland_gyermekporno.html
[utolsó megtekintés: 2012.09.30.]

23) **ILLÉSI Zsolt**: Hackers beware! – Digitális nyomok az informatikai rendszerekben
Hacktivity 2009, [Online], 2009.
https://hacktivity.com/hu/letoltesek/archivum/105/
[utolsó megtekintés: 2012.09.30.]

24) **HAIG Zsolt, VÁRHEGYI István**: Hadviselés az információs hadszíntéren
Zrínyi Kiadó, Budapest, 2005.
ISBN 963 327 391 9

25) **HAIG Zsolt**: Számítógép–hálózati hadviselés rendszere az információs műveletekben
in Bolyai Szemle, Vol. 1. szám.
ZMNE, Budapest, 2006.
http://portal.zmne.hu/download/bjkmk/bsz/bszemle2006/1/06_Haig_Zsolt.pdf
ISSN: 1416–1443
[utolsó megtekintés: 2012.09.30.]

26) **VARGA Péter**: Rádiós hálózatok elleni támadások rendszertana
in Robothadviselés 10.
ZMNE, Budapest. 2010.11.24.
http://robothadviseles.hu/program_rw10.html
[utolsó megtekintés: 2012.09.30.]

27) **GYÁNYI Sándor**: Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem PhD értekezés
ZMNE: Budapest, 2012.

28) **HAIG Zsolt, KOVÁCS László**: Fenyegetések a cybertérből
ZMNE, 2008.
ISSN 1789–5286

29) **ANONYMUS HACKER GROUP**, Facebook, [Online]
http://www.facebook.com/pages/Anonymus-Hacker-Group/115842198427000
[utolsó megtekintés: 2012.09.30.]

30) **Severino H. GANA**: Prosecution of cyber crimes through appropriate cyber legislation in the Republic of the Philippines
Asia Crime Prevention Foundation (acpf.org), [Online],
[Az eredeti weblapot 2008.02.06. mentette le a WayBack Machine internet archívum; eredeti url:
http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana,Phillipine.html]
arcív url:
http://web.archive.org/web/20080206114348/http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana,Phillipine.html
[utolsó megtekintés: 2012.09.30.]

31) **KOVÁCS László, ILLÉSI Zsolt**: Cyberhadviselés
in Hadtudomány XXI. évfolyam 1–2. szám, pp. 29–41
ZMNE, Budapest, 2011. május
ISSN 1215–4121

32) **KOVÁCS László**: Cyber terrorizmus
Hadtudományi Doktori Iskola, [Online], 2006.
http://www.zmne.hu/dokisk/hadtud/terror/lekt_Kovacs_Laszlo.pdf
[utolsó megtekintés: 2012.09.30.]

33) **KOVÁCS László**: Az információs terrorizmus eszköztára
Hadmérnök, Robothadviselés 6. 2006. november 22. különszám
ZMNE, Budapest, 2006. november
ISSN 1788–1919

34) **ILLÉSI Zsolt**: Botnetek kialakulása, használatuk, trendjeik
in Hadmérnök. III. évfolyam, 2. szám, pp. 129–137
ZMNE, Budapest, 2008 június
ISSN 1788–1919

35) **N.PAULAUSKAS, E.GARSVA**: Computer System Attack Classification
Electronics and Electrical Engineering, [Online], 2006.
http://www.ee.ktu.lt/journal/2006/2/1392-1215-2006-02-66-84.pdf
ISSN 1392–1215
[utolsó megtekintés: 2012.09.30.]

36) **ILLÉSI Zsolt**: Information violation (?) and computer forensics
Óbudai Egyetem, Budapest: 2011.11.19.
ISBN 978–615–5018–20–6

37) **MUNK Sándor**: Katonai Informatika a XXI. század elején
Zrínyi Kiadó, 2007.
ISBN 978–963–327–419–4

38) **NAGY Zoltán András**: Bűncselekmények számítógépes környezetben
Ad Librum, Budapest: 2009.
ISBN 978–963–9888–92–0

39) **BALOGH Zsolt György**: Jogi informatika
Dialóg Campus Kiadó,Budapest-Pécs, 1998.
ISBN 963–9123–19–6

40) 1978. évi IV. törvény a büntető törvénykönyvről

41) **TREMMEL Flórián**: Bizonyítékok a büntetőeljárásban
Dialóg Campus Kiadó, Budapest-Pécs, 2006.
ISBN 963–7296–72–7

42) **KENGYEL Miklós** (szerk.): A polgári perbeli bizonyítás gyakorlati kézikönyve
KJK Kerszöv Jogi és Üzleti Kiadó Kft., Budapest, 2005.
ISBN 963 224 862 7

43) 1952. évi III. törvény a polgári perrendtartásról

44) 1998. évi XIX. törvény a büntetőeljárásról

45) **KIRÁLY Tibor**: Büntetőeljárási jog
Osiris Kiadó, Budapest, 2008.
ISBN 978–963–276–005–6

46) **ÁDÁM György**: Bizonyítás a polgári peres eljárásban
Lege & Artis – Magyar bírósági határozatok jogelméleti elemzése, [Online], 1999.08.20.
http://www.jog-vita.hu/bizonyitas.html
[utolsó megtekintés: 2012.09.30.]

47) **TREMMEL Flórián, FENYVESI Csaba**: Kriminalisztikai Tankönyv és Atlasz
Dialóg Campus Kiadó, Budapest-Pécs, 2002.
ISBN 963–85756–8–9

48) **BÓCZ Endre** (szerk.): Kriminalisztika 1–2
BM Kiadó, Budapest, 2004.
ISBN 963–8036–84–2

49) **Wayne JANSEN, Rick AYERS**: Guidelines on Cell Phone Forensics – Recommendations of the National Institute of Standards and Technology. Computer Security Division Information Technology Laboratory,
NIST Special Publication 800–101
NIST, [Online], 2007.05.
http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf
[utolsó megtekintés: 2012.09.30.]

50) **Eoghan CASEY**: Digital Evidence and Computer Crime – Forensics Science, Computers and the Internet, Second Edition
Academic Press, UK, 2004.
ISBN-13: 978–0–12–163104–8

51) **POKÓ István**: Digitálisnyom-elemző rendszer
Networkshop 2011, Kaposvár, 2011. április 27-29.

52) **PESZLEG Tibor**: Interneten, számítógépen történő nyomrögzítés
in Ügyészek lapja 12. évf. 1. sz., pp. 25–40
Ügyészek Országos Egyesülete, 2005.
ISSN 1217–7059

53) **MSZ ISO/IEC** 15408–2: Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai 2. rész: A biztonság funkcionális követelményei. 2003. március

54) **Network Working Group**: Guidelines for Evidence Collection and Archiving (RFC: 3227)
The Internet Engineering Task Force (IETF), [Online], 2002.02.
http://www.ietf.org/rfc/rfc3227.txt
[utolsó megtekintés: 2012.09.30.]

55) **UNICSOVICS György**: Szteganográfia elemeinek implementálási lehetőségei a védelmi szektorban (PhD értekezés)
ZMNE, Budapest, 2007.

56) **Linda VOLOMINO, Reynaldo ANZADULA**: Computer forensics for dummies
Wiley Publishing Inc., USA, 2008.
ISBN 978–0–470–37191–6

57) **TAKÁCS Péter, RAJNAI Zoltán**: WiFi hálózatok veszélyei
in Hadmérnök, pp. 359–361
ZMNE, Budapest, 2007.
ISSN 1788–1919

58) **ILLÉSI Zsolt**: WiFi hálózatok igazságügyi szakértői elemzése:
WiFi hálózatok felderítése
in Hadmérnök IV. évfolyam, 3. szám, pp. 285–302
ZMNE, Budapest, szeptember 2009.
ISSN 1788–1919

59) **ILLÉSI Zsolt**: Open source IT forensics – avagy nyílt forráskódú programok felhasználása az informatikai igazságügyi szakértésben
in Bolyai Szemle, XVII. évfolyam, 4. szám, pp. 181–195
ZMNE, Budapest, 2008.
ISSN: 1416–1443

60) **U.S. Department of Justice**: Forensics Examination of Digital Evidence:
A guide for Law Enforcement
National Criminal Justice Reference Service (NCJRS), [Online], 2004.04.04.
www.ncjrs.gov/pdffiles1/nij/199408.pdf
[utolsó megtekintés: 2012.09.30.]

61) **Altheide CORRY, Carvey HARLAN**: Digital Forensics with Open Source Tools
Syngress, U.S., 2011.
ISBN 978–1–59749–586–8

62) **Brian CARRIER**: Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers
Scientific Literature Digital Library and Search Engine, [Online], 2003.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.9813&rep=rep1&type=pdf
[utolsó megtekintés: 2012.09.30.]

63) **Brian CARRIER**: File System Forensic Analysis
Addison-Wesley, USA, 2008.
ISBN 0–321–26817–2

64) **ILLÉSI Zsolt**: Számítógép-hálózatok kriminál technikai vizsgálata
in Hadmérnök, IV. évfolyam, 4. szám, pp. 163–175
ZMNE, Budapest, 2009. december
ISSN 1788–1919

65) 9/2006. (II. 27.) IM rendelet az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről

66) **U.S. Department of Justice, Federal Bureau of Investigation Laboratory Division**: Handbook of Forensic Services
The Federal Bureau of Investigation (FBI), [Online], 2007.
http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf/at_download/file
ISBN 978–0–16–079376–9
[utolsó megtekintés: 2012.09.30.]

67) **ILLÉSI Zsolt:** Tűt a szénakazalban
Hacktivity, [Online], 2010.
https://hacktivity.com/hu/letoltesek/archivum/47/
[utolsó megtekintés: 2012.09.30.]

68) **DETERKŐI Ákos, SZABÓ György**: Bevezetés a térinformatikába
Nemzeti Tankönyvkiadó, Budapest, 1995.
ISBN 963 18 8397 3

69) **Laura CHAPPELL**: Wireshark Network Analysis – The Official Wireshark Certified Network Analyst Study Guide.
Chappel University, U.S., 2010.
ISBN 978–1–893939–99–8

70) **Debra LITLEJOHN SHINDER**: The Scene of the Cybercrime – Computer Forensics Handbook
Syngress Publishing, USA, 2002
ISBN 1–931836–65–5

71) **EC-Council**: Computer Hacking Forensic Investigator, Vols. 1–4, Version 4.
EC-Council U.S.

72) **Microsoft**: Fundamental Computer Investigation Guide for Windows
Microsoft Download Center, [Online], 2007.
http://technet.microsoft.com/en-us/library/cc162846.aspx
[utolsó megtekintés: 2012.09.30.]

73) **Martin, ANTONIO**: FireWire Memory Dump of a Windows XP Computer: A Forensic Approach. Security Things – Current and Future Security Issues and Trends,
[Online], 2007.
http://www.friendsglobal.com/papers/FireWire%20Memory%20Dump%20of%20Windows%20XP.pdf
[utolsó megtekintés: 2012.09.30.]

74) **hackaholic.org**: Anti forensics: making computer forensics hard
[Online],
http://dl.packetstormsecurity.net/papers/bypass/antiforensics.pdf
[utolsó megtekintés: 2012.09.30.]

75) **NIST**: Guidelines on PDA Forensics.
Computer Security Division Information Technology Laboratory
NIST, [Online], 2004.
http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf
NIST Special Publication 800–72
[utolsó megtekintés: 2012.09.30.]

76) **Diane BARRETT, Gregory KIPPER**: Virtualization and Forensics –
A Digital Forensic Investigator's Guide to Virtual Environments
Syngress, U.S, 2010.
ISBN 978–1–59749–557–8

77) **forensicswiki.org**: File Carving
[Online]
http://www.forensicswiki.org/wiki/File_Carving
[utolsó megtekintés: 2012.09.30.]

78) **CARVEY, Harlan**: Windows Forensic Analysis
Syngress, U.S., 2009.
ISBN 978–1–59749–422–9

79) **MORRISSEY, Sean**: iOS Forensic Analysis for iPhone, iPad, and iPodTouch
Apress, U.S., 2010.
ISBN 978–1–4302–3342–8

80) **ILLÉSI Zsolt**: Rádiós hálózatok kriminál technikai vizsgálata
in 2009. XXV. Nemzetközi Kandó Konferencia kiadványa
Óbudai Egyetem, Budapest, 2009.
ISBN 978–963–7158–04–9

81) **ILLÉSI Zsolt**: Computer forensics need for a domestic and/or EU 'hash factory'
in XX VI. Nemzetközi Kandó Konferencia kiadványa
Óbudai Egyetem, Budapest, 2010.11.04.
ISBN 978–963–7158–04–9

82) **Jan GOYVAERTS**: Email Addresses: The Official Standard: RFC 2822
Regular-expressions Info, [Online]
http://www.regular-expressions.info/email.html
[utolsó megtekintés: 2012.09.30.]

83) **ILLÉSI Zsolt**: NEEDLE IN A HAYSTACK –
A Quest to Identify, Classify, and Reduce Data to Find Adequate Digital Evidence
in VIII Konferencija Naukova Studentóv 8th Students konference, pp. 275–281.
Oficína Wydawnicza Politechniki Wroclawskiej, Wroclaw, Poland, 2010.
ISSN 1732–0240

84) 1995. évi CXIV. törvény az igazságügyi szakértői kamaráról

85) 2005. évi XLVII. törvény az igazságügyi szakértői tevékenységről

86) **ILLÉSI Zsolt**: Az igazságügyi szakértés modellezése
in Hadmérnök, V. évfolyam 4. szám, pp. 122–132
ZMNE, Budapest, 2010.
ISSN 1788–1919

87) **John ASCHCROFT, Deborah J. DANIELS, Sarah V.HART**: Forensics Examination of
Digital Evidence: A guide for Law Enforcement
www.nij.gov, [Online],
http://www.ncjrs.gov/pdffiles1/nij/199408.pdf
NCJ 199408
[utolsó megtekintés: 2012.09.30.]

88) **KATONA Géza**: Bizonyítási eszközök a XVIII-XIX. században –
A kriminalisztika magyarországi előzményei
Közgazdasági és Jogi Könyvkiadó, Budapest, 1977.
ISBN 963–220–514–6

89) **SZÁNTÓ I. József**: Igazságügyi szakértői ismeretek I.
- A szakértői bizonyítás alapjai
Dunatrend-Press, Budapest, 1999.
ISSN 1585–325X

90) **NYÍRI Sándor**: A titkos adatszerzés
BM Kiadó, Budapest, 2000.
ISBN 963–8036–53–2

91) **HARGITAI József**: Jogi Fogalomtár
Magyar Hivatalos Közlönykiadó, Budapest, 2005.
ISBN 963–9221–6–7.

92) **FINSZTER Géza**: A kriminalisztika elmélete és a praxis
a büntetőeljárási reform tükrében
[Online], 2005–2007.
http://users.atw.hu/be/letoltes/Krimjegyzet.doc
[utolsó megtekintés: 2012.09.30.]

93) **Zakaria ERZINÇLIOGLU**: Helyszínelők –
A törvényszéki vizsgálatok képes útmutatója
Pécsi Direkt Kft. Alexandra Kiadója, Pécs, 2006.
ISBN 963–369–983–5

94) **PESZLEG Tibor**: A digitális bizonyítási eszközök megszerzésének elvei
és gyakorlati érvényesülésük
in Ügyészek Lapja, Vol. 2, pp. 23–32
Ügyészek Országos Egyesülete, Budapest: 2010.
ISSN 1217–7059

95) **Richard PLATT**: Tettesek és tetthelyek – Munkában a bűnügyi helyszínelők
Aréna Kiadó, Budapest, 2006.
ISBN 963–704669–0

96) **DÓSA Imre** (lekt.): Az informatikai jog nagy kézikönyve
CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2009.
ISBN 978–963–224–963–6

97) **Robert A. MAKSIMSCHUK, Eric J. NAIBURG**: UML földi halandóknak
Kiskapu Kft., Budapest, 2006.
ISBN 963–9637–14–9

98) **BÓCZ Endre, FINSZTER Géza**: Kriminalisztika joghallgatóknak
Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2008.
ISBN 978–963–9722–39–2

99) **SZABÓ József** (szerk.): Hadtudományi Lexikon (I–II. kötet)
Magyar Hadtudományi Társaság, Budapest, 1995.
ISBN 963 04 5226 X

TÁBLÁZATOK JEGYZÉKE

ÁBRÁK JEGYZÉKE