HADMÉRNÖK

IV. Évfolyam 4. szám - 2009. december

Illési Zsolt
illesi.zsolt@proteus.hu

SZÁMÍTÓGÉP HÁLÓZATOK KRIMINÁLTECHNIKAI VIZSGÁLATA

Absztrakt

Az infokommunikációs technológia (ICT) átitatja a mindennapokat a „virtuális" megoldások egyre több teret nyernek a hagyományos megoldásokkal szemben. Ezzel párhuzamosan nőtt az ICT szerepe a bűnözésben is. A bűncselekmények széles körének vizsgálatakor az ICT eszközök büntetőjogilag releváns információkat (bizonyítékokat) hordoznak, így bizonyítékforrásként célszerű ennek a szektornak a kriminalsztikai, kriminálltechnikai vizsgálatával foglalkozni. Az ICT kriminálltechnikai vizsgálata új kutatási módszereket és technikákat igényel. A cikk ennek a megközelítésére javasol egy módszert, amely Brian Carrier réteg megközelítésére épül, és amely alkalmas a szakmai kompetenciák meghatározására és az együttműködés interfészeinek azonosítására.

Infocommunication technology (ICT) is impregnated into the everyday life, and the "virtual" solutions are gaining around with traditional technologies. In parallel, increases the role of ICT in crime. Investigating the wide range of criminal activities the ICT equipments may provide relevant information from criminal law point of view (evidence), therefore it is practical to deal with criminal study and forensic analysis of this sector as a source of evidence. Forensic analysis of ICT requires new research methods and techniques. This paper proposes a method, based on Brian Carrier's abstraction layer approach, to this analysis, and also suitable for professional competence and identifying the interfaces of cooperations.

Kulcsszavak: *számítógép hálózatok, informatikai rendszerek vizsgálati rétegei, kriminálltechnikai vizsgálatok ~ computer networks, investigation layers of information systems, forensics analysis*

Bevezetés

Az informatika az infokommunikációs technológia a mindennapok megszokott részévé vált. Hazánkban 1,2[1] az egy főre eső mobiltelefonok száma; szinte minden háztartásban van már számítógép; valamennyi diák számára elérhető az internet. Sőt! A szélessávú internet hozzáférést néhány EU tagország már alapvető emberi jogként deklarálta.[2]

A számítógépek, az infokommunikáció jelen van a háztartásokban, az iskolákban, a kutatóhelyeken, a munkahelyeken. Az informatika, a telekommunikáció elmaradhatatlan részéivé vált a mindennapjainknak.

Az infokommunikációs eszközök azonban nem egymástól elszigetelten működnek, hanem hálózatokba rendezve kapcsolódnak és megosztják egymással az erőforrásaikat, támogatják a beépített funkciókat, lehetővé teszi az alkalmazások távoli elérését és használatát.

Az intenzív használat, az „up-to-date"adatforrások és a hatékonyság és eredményesség növelő funkciók minden használó számára kívánatosak és hasznosak. Azonban a jogkövető felhasználók mellett az infokommunikációs eszközök és technológia magához vonzotta a bűnelkövetőket – köztük a terroristákat – is. Az egyedi számítógépek, hálózati eszközök, de maga a hálózat (függetlenül a kiterjedésétől) lehet:

- célpont,
- megvalósítási/ elkövetési tárgy/ környezet,
- elkövetés szimbóluma,
- elkövetés „tanúja".

[2][6][9]

A fentiek miatt a számítógép hálózatok, mint az infokommunikációs technológia egyik működési területe, jó bizonyítékforrássá válhatnak, így tárgyai lehetnek a kriminalisztikának, azon belül a krimináltechnikai vizsgálatoknak.

Az infokommunikáció egy rendkívül gyorsan változó, bővülő tudományterület. A nyomfelderítést, a helyszíni nyomrögzítést, a titkos nyomozást a nyomozóhatóság képviselői látják el, akik véletlenszerű tartalmú és mélységű informatikai szakismerettel rendelkeznek és nincs napi rutinjuk, mély és formális ismeretük az informatikai és a telekommunikáció terén. A rögzített nyomok értékelését azonban – formális képzésben szerzett ismeretekkel, szakértelemmel és a speciális szakmai gyakorlattal rendelkező – igazságügyi szakértők végzik el, akiknek az ismeretei heterogének. Mindezek miatt célszerű a számítógép hálózatok, mint lehetséges bizonyítékforrásoknak a tudományos kutatása, a nyomfelkutatási, nyomrögzítési, esemény rekonstrukciós és elemzési tevékenységeit (a számítógép hálózat krimináltechnikai vizsgálat területét) tanulmányozni. A kutatás eredménye egy olyan megközelítés – módszerek és technikák együttese – lehet, amely alapul szolgálhat a nyomozóhatóság és az érintett igazságügyi szakértők kompetencia alapú professzionális feladatvégzésének és együttműködésük meghatározásának.

A cikkben ismertetni szeretnék egy, a számítógép hálózatok krimináltechnikai

[1] http://portal.ksh.hu/pls/ksh/docs/hun/xftp/gyor/tav/tav20903.pdf

[2] http://eziнearticles.com/?Internet-Access-As-a-Human-Right&id=3243554
http://www.foxnews.com/story/0,2933,525993,00.html
http://www.csmonitor.com/2003/0701/p07s01-woeu.html
http://www.vouli.gr/politeuma/syntagmaDetails.asp?ArthroID=6
http://translate.google.hu/translate?js=y&prev=_t&hl=hu&ie=UTF-8&u=http%3A%2F%2Fwww.vouli.gr%2Fpoliteuma%2FsyntagmaDetails.asp%3FArthroID%3D6&sl=el&tl=hu
http://index.hu/tech/2009/10/19/allampolgari_jog_lett_a_szeles_sav_finnorszagban/

vizsgálati megközelítésére alkalmas modellt, amely kiindulópontja lehet egy igazságügyi módszertani levélnek.

1 Kriminál technikai vizsgálatokról általában

1.1 A kriminalisztikai vizsgálatok célja

A kriminalisztikai vizsgálatoknak, ezen belül a kriminál technikai vizsgálatok célja a törvényes forrásból származó, büntetőjogilag releváns tények szolgáltatása, amelyek összességükben alkalmasak büntetőjogilag releváns tényállás megállapítására. {[10] 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?).

{[11] p. 58-59.}

A vizsgálatokat a fenti kérdésekre figyelemmel kell előkészíteni, hogy azok adekvát válaszokat adjanak és közvetett vagy közvetlen bizonyítékot szolgáltassanak. [8][10]

1.2 A számítógép hálózat kriminál technikai vizsgálati megközelítése

Az informatikai rendszerek vizsgálatakor lényeges szempont, hogy milyen körülmények között, milyen eszközökkel és mikor zajlik a vizsgálat.

A szakirodalomban elterjedt az élő-holt rendszer felosztás. Az élő rendszer e szerint a felosztás szerint azt jelenti, hogy a vizsgálatot a vizsgálni kívánt számítógépen, annak operációsrendszerét és segédprogramjait felhasználva végezzük. A holt rendszer, ezzel ellentétben azt jelenti, hogy a vizsgálatot saját megbízható eszközökkel, saját megbízható környezetben végezzük. Ez utóbbi megközelítés megbízhatóbb eredményt szolgáltat ugyan, de a valóságban 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 kriminál technikai szakirodalma azonban nem ilyen módon osztja fel a vizsgálatokat, hanem a számítógép hálózatokból kinyerhető adatforrások szerint írja le a vizsgálati folyamatot:

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

{[7] p. 241-263.}

A másik megoldás a számítógép hálózatok IP protokoll, vagy ISO/OSI réteg alapú megközelítése. {[4] p. 370-380.}

Véleményem szerint az élő-holt megközelítés kiegészítésre szorul, mivel nincs tekintettel az elkövetés és a vizsgálat időbeni kapcsolatára (egyidejű vagy követő vizsgálat), illetve nem eléggé pontosan határolja el a vizsgált eszköznek és környezetnek a vizsgálatra gyakorolt befolyását. A fenti felosztások közül a második a kriminál technikai vizsgálatok leírására nem alkalmas mivel a fókuszban csak a hálózati rétegek állnak, a bizonyítékok megszerzésének módjáról és időzítéséről nem szól. Javaslok egy olyan megközelítést, amely az élő-holt felosztáshoz hasonlít leginkább, de javaslom azt tovább finomítani az alábbiak szerint:

- az elkövetés-vizsgálat időbenisége szerint:
  - az elkövetéssel egyidejű
  - az elkövetés után végzett
- vizsgált rendszer működési állapota szerint:
  - kikapcsolt (holt)
  - bekapcsolt (élő)
- a vizsgáló eszköz (program) kontrollja szerint:
  - a vizsgált rendszerbe integrált (a vizsgált rendszer kontrollja alatt álló)
  - a vizsgált rendszertől független (a vizsgált rendszernek nincs kontrollja a vizsgáló felett)

A cikkben a számítógép hálózatoknak az elkövetéssel egyidőben végzett kriminál technikai vizsgálatával (nyomrögzítés és elemzés) foglalkozom, amikor is a vizsgálat tárgya (a hálózat) működik, függetlenül attól, hogy az adatgyűjtést végző eszköz a vizsgálati környezet kontrollja alatt áll-e vagy sem.

1.3 Locard anyagcsere és kölcsönös nyomhagyási szabálya

A számítógép hálózatok kriminál technikai vizsgálatának meg kell felelnie a kriminalisztika általános követelményeinek és az infokommunikációs rendszerek sajátosságainak is.

Az elsődleges alapelv, amely a kriminál technikai vizsgálatokat megalapozza Edmond Locardtól, az 1920-as évek kiemelkedő kriminalisztikai szakértőjétől származik. Alapelve (Locard Exchange Principle) szerint bárki, vagy bármi kerül kapcsolatba egy bűncselekmény helyszínével valamilyen nyomot hagy és valamilyen nyomot tovább visz magával, amikor elhagyja azt. Az elv következetes alkalmazása vezetett a traszológia (nyomtan) kifejlődéséhez, és ez alapján lehet az elkövetőt, a sértettet és a tetthelyet összekapcsolni és a kapcsolódásra utaló nyomokat a büntetőeljárásban felhasználni.

A kriminalisztika és a traszológia egyik alapfogalma a nyom, hiszen ez az, amit megfelelő szakértelemmel végzett elemzést követően a büntetőeljárásban büntetőjogilag releváns tényként valamilyen állítás igazolásához vagy cáfolatához bizonyítékként fel lehet használni. A nyom helyes kategorizálása az alapja annak, hogy azokat megfelelően azonosítani, konzerválni és elemezni lehessen.

A nyom a jelenlegi értelmezés szerint lehet lenyomat (valamilyen tárgy morfológiai sajátságait magán viselő nyom, ilyen lehet például egy ujjnyom, törésnyom, lövedéken a huzagolás miatt keletkezett elváltozások), de lehet anyagmaradvány is (valamilyen anyag kémiai, biológiai sajátosságait magán viselő nyom, például vér, DNS, anyagmaradvány, amelynek az összetétele lényeges). A nyomok vizsgálata során sokszor előfordul, hogy ugyanaz a nyom mindként fenti kategóriába beletartozik és csak a vizsgálati eljárás sajátosságai használják ki ezen nyomok lenyomat-anyagmaradvány természetét, például egy ajaklenyomat és a lenyomatról vett nyál/DNS minta kettős természetű vizsgálatakor.

Véleményem szerint a fenti két nyom-kategória az infokommunikációs rendszerekben keletkező nyomokra nem alkalmazható. Szükségesnek tartom egy harmadik kategória bevezetését, a digitális nyomét, vagy másként az „adatmaradvány”-ét. [5][8]

1.4 Az infokommunikációs rendszerből kinyert bizonyítékok osztályozása

Az infokommunikációs rendszerből (így a számítógép hálózatból) 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 számítógép hálózat továbbá irreverzibilis bizonyítékforrás, mivel az azon áthaladó jelek csak egyszer léteznek, csak akkor és ott (ex tunc et allicundo) vizsgálhatók.

A számítógép hálózatokból kinyert bizonyítékokról megállapítható, hogy mind az elkövetés tárgyi oldaláról (in rem), mind pedig a személyi oldaláról (in personam) szolgáltat információkat.Meg kell azonban jegyeznem, hogy a számítógép hálózatokból kinyert bizonyíték elsősorban in rem bizonyítékforrás, csak ritkán (például az elkövetésről készült jó minőségű on-line továbbított videó felvétel, vagy hálózaton keresztüli biometriai azonosítás esetén a küldött/fogadott biometriai adatok) szolgáltat in personam bizonyítékokat. Ez a sajátos hangsúlyeltolódás egyébként az infokommunikációs rendszerek kriminál technikai vizsgálatainak egészére igaz, és sajátos többlet nyomozati feladatokat generál az in rem bizonyítékok természetes személyhez kötésénél[3].
[8][10]

1.5 Daubert kritériumok

A bizonyítékgyűjtés nem lehet minden kontroll nélküli. Ha nincsenek korlátai a bizonyításnak, akkor az teret adhatna a korlátlan megfigyelésnek, az alaptalan bizonyítékok felhasználásának 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 Büntetőeljárási törvény (1998. évi XIX. törvény a büntetőeljárásról, a továbbiakban Be./ [1]) 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 publikált-e, mi a tudományos elemzésének eredménye (megmutatható-e a hamissága, tehát falszifikálható-e, cáfolhatóság, tesztelhetőség[4]), és a szakemberek közössége által elismert-e,
- keresztül ment-e alapvető gyakorlati teszteken. [6][8]

[3] A felhasználói név nem azonos a felhasználóval magával. Azonos felhasználói név alatt többször több személy egymástól függetlenül is tevékenykedhet, még az sem biztos, hogy a jogosult felhasználó tudtával, vagy anélkül történik-e mindez. Tehát valamilyen felhasználói név alatt elkövetett cselekmény önmagában még nem alapozza meg a felróhatóságot. Bizonyítandó, hogy a terhelt használta az adott eszközt az elkövetés idején.

[4] Ld. Karl Raimund Popper osztrák és Lakatos Péter magyar tudományfilozófusok munkáit.

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. azonban nem említi meg a „tudományosság” kritériumát a nyomozóhatóság nyomozati feladataival kapcsolatban. Figyelembe véve azonban, hogy amatőr módon, megalapozatlan eljárásokkal végzett nyomrögzítés – ami a kriminál technikai vizsgálatok kezdő lépése – nem szolgáltathat szakszerű, tudományos szakvélemény alapjául. Ezért a Daubert kritériumok betartása 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. [1]

1.6 Logikus érvelés és Occam borotvája

Az egyes bizonyíték elemek megszerzésének tehát ki kell állniuk a tudományosság próbáját. A bizonyítás során hangsúlyt kell helyezni a logikus érvelésre, az ok-okozati lánc fenntartására, kerülendő az inkonzekvens következtetés.

Az indíciumoknak a bizonyítandó feltételezést alátámasztó láncolatának azonban nem csak logikusnak, de egyszerűnek kell lennie. A lehetséges verziók felállításakor kerülni kell az oda nem való részletekkel való kiegészítést, használni kell Occam borotváját, hogy a rendelkezésre álló indíciumok alapján a legvalószínűbb magyarázattal szolgálhasson.

A bizonyítás során lényeges, hogy a bizonyíték a bizonyítandó feltevés alátámasztásán túl alkalmas legyen az alternatív feltevések kizárására. [5][6][8]

2 A számítógép hálózatok vizsgálati modellje

Számítógép hálózatnak azt a speciális infokommunikációs alrendszert tekintem, amely a számítógépek kommunikációs eszközök egymás közötti kommunikációját biztosítja. A számítógép hálózat kategorizálható a mérete, a funkcionális kapcsolatok, a topológiája, az adatátviteli sebesség szerint. [12]

A kriminál technikai vizsgálatok szempontjából a számítógép hálózat egyszerűsített sémája a következő:

1. ábra – Számítógép hálózatok egyszerűsített sémája
[szerkesztette: Illési Zsolt]

A sémában szereplő

- hálózat az átviteli közeget, a csatorna kódolást, valamint a hálózati adatforgalomban szerepet játszó aktív hálózati eszközöket (jeltovábbítás esetén),
- végpont az adatforrásokat és nyelőket jelentik, amik szerverek, munkaállomások vagy aktív hálózati eszközöket („saját jogon” történő kommunikáció esetén).

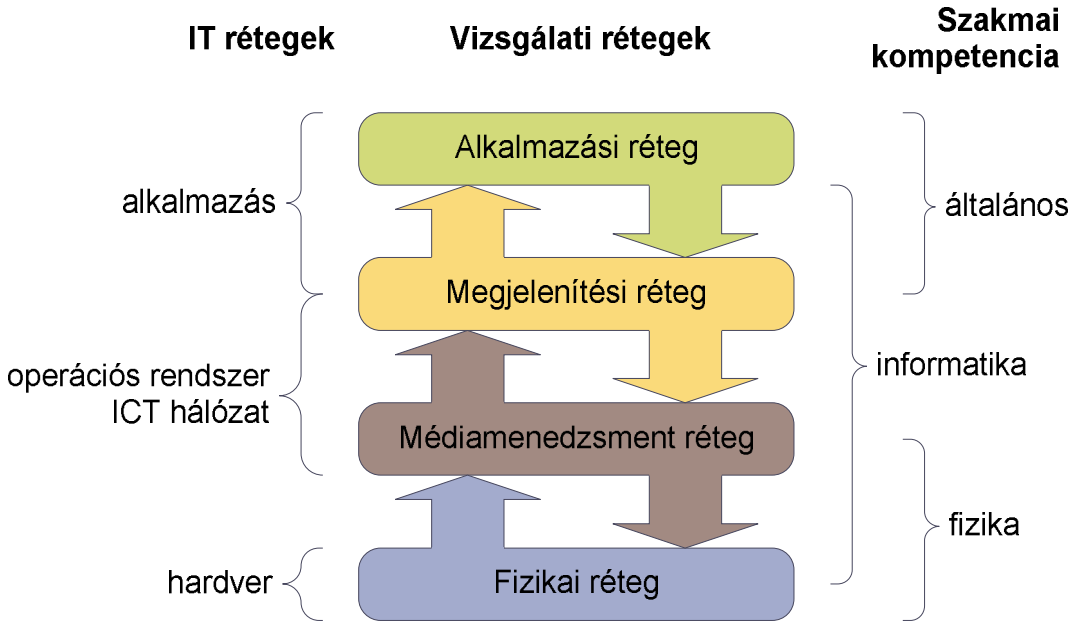
A cikkben nem foglalkozom a hálózati végpontokon és aktív hálózati eszközökön tárolt

adatokkal, naplóállományokkal, vezérlési logikák vizsgálatával, sem ezen eszközök és működési paramétereik felderítésének kérdéseivel; de nem foglalkozom az általános infokommunikációs eszközökről kriminalisztikai célból történő adatszerzéssel sem. Ezek a vizsgálatok nem tartoznak közvetlenül a számítógép hálózat – pontosabban a számítógép hálózati adatforgalom – vizsgálatának a tárgykörébe.

A fenti számítógép hálózati séma azonban még nem elegendő ahhoz, hogy az azon történő adatforgalom vizsgálatát modellezni lehessen, továbbá még nem ad kellő információt arról, hogy a kriminálltechnikai vizsgálatok során milyen feladatokat kell ellátni és ezekhez milyen speciális szakértelem szükséges.

Brian Carry 2003-ban publikált egy réteg megközelítést, amelyet ő az adathordozók vizsgálatának elemzéséhez használt. [3] Az ő réteg-megközelítése a számítógép hálózatokra, mint a modellbe nem illeszkedő, attól eltérő entitásokra tekint. Véleményem szerint Brian Carry modellje megfelelő kiegészítésekkel alkalmassá tehető az infokommunikációs eszközök és rendszerek kriminálltechnikai vizsgálatának általános leírására, illetve alapjául szolgálhat az egyes rétegekkel kapcsolatos kriminalisztikai funkciók meghatározására, továbbá e funkciók megvalósításához szükséges szakértelem és az egyes szakterületek közötti interdependencia azonosítására.

Brian Carry modellje az általam tett kiegészítésekkel a következő:



2. ábra – Informatikai rendszerek vizsgálati rétegei
[forrás: [3] alapján szerkesztette: Illési Zsolt]

2.1 Fizikai réteg

A fizikai réteggel kapcsolatos tevékenységek célja a számítógép hálózaton áthaladó valamennyi, az ügy szempontjából releváns jel érzékelése, rögzítése, a rögzített adatok időpecséttel, ellenőrző kóddal (hash), esetleg digitális aláírással való hitelesítése. A későbbi vizsgálati lépések (keresés és elemzés) szempontjából ez alapvető fontosságú. A hiányos bitminta gátja lehet az adatok rekonstruálásának, mivel a számítógép hálózaton továbbított jelek 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 valódisága, ezért bizonyítékként való felhasználhatósága jelentősen csökkenhet, vagy 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 tehát speciális szaktudásra van szükség a fizika, a villamosmérnöki, és az információ- és kódelmélet terén.

Az elkövetéssel egyidőben végzett hálózati adatforgalom rögzítése 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, szükség esetén bevonva az adattovábbítást végző szervezet képviselőit. A jelenleg hatályos Be. nem szól a különleges szakértelemmel rendelkező személyek (nem szakszolgálati szakértők) szükséges szerepéről a titkos adatszerzés során. [1]

Mivel a szakszolgálatok és a nyomozóhatóságok alapvetően nem 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, illetve 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, mivel egy (telekommunikációs, számítógép hálózati) szakmai szempontból laikus szervezetnek kell egy általa csak részben vagy nem ismert terület szabályinak betartásáról, betartatásáról gondoskodnia.

Véleményem szerint ilyen estekben a titkos adatgyűjtést végző szervezetnek igazságügyi szakértőt kellene kirendelnie szaktanácsadóként a nyomrögzítés elvégzésére, vagy a nyomrögzítés szakmai feltételeinek felügyeletére. A probléma részben kezelhető azonban, mivel a hálózati adatforgalom rögzítése elterjedt hálózati technológiák esetén alkalmas hardver és szoftver segítségével automatizálható. Sokat segítene ebben a kérdésben (is), ha ilyen típusú vizsgálatokkal, nyomrögzítéssel kapcsolatos módszertani levelek megszületnének és egységesen kiadásra kerülnének a nyomozóhatóságok, a szakszolgálatok és az igazságügyi szakértői kamara tagjai számára.

2.2 Médiamenedzsment réteg

A számítógép hálózat krimináltechnikai vizsgálatának második lépcsője során a cél a fizikai réteg elemzését, az azon áthaladó bitfolyam rögzítését követően az elsődleges adat-konténerek (a hálózati keretek) azonosítása és elkülönítése egymástól.

Az egyik szakmai problémát az jelenti, hogy a bitfolyam elvileg többféleképpen értelmezhető, az egységes (valamennyi kódolási eljárásban egységesen alkalmazott) irreducibilis kódok használata nem jellemző. Amennyiben a hálózati keretek nem különíthetők el egyértelműen egymástól, úgy az alkalmazott hálózati csomagok, hálózati protokollok, protokoll hierarchiák mélyebb ismeretére, illetve minta illesztő 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 APR csomag kezdete

3. ábra – ARP csomag lehetséges értelmezése egy bitfolyamban
[szerkesztette: Illési Zsolt]

A médiamenedzsment rétegben kell először a csatorna-dekódolás esetleges hibáit, zavarait is figyelembe venni, ebben is a protokoll hierarchia mélyebb ismerete (alkalmazott hibafelismerő és hibajavító kódolás) szükséges.

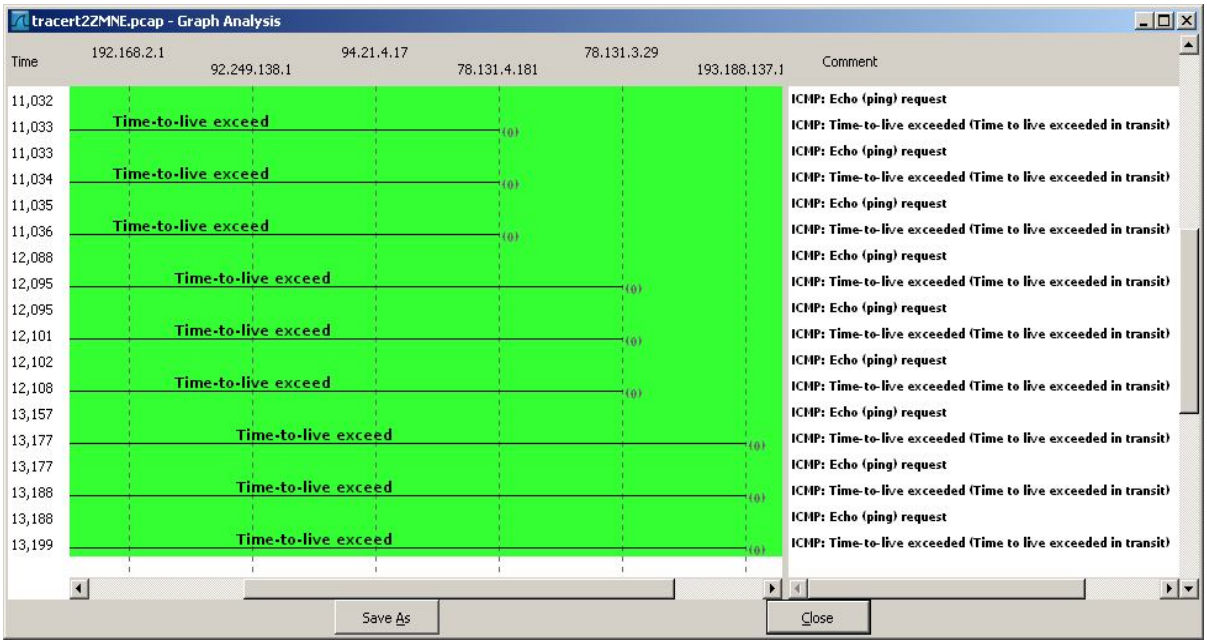
2.3 Megjelenítési réteg

A megjelenítési rétegbeli vizsgálatok célja az adatkeretek belső szerkezetének a feltárása, a protokoll információk dekódolása, a hálózati protokoll hierarchia „visszafejtése” és az átvitt adatok (email, dokumentumok, felkeresett weblapok, távoli rendszerekben kiadott parancsok, programok stb.) összeállítása, a hálózati események időbeli sorrendjének rekonstruálása.

Az adatkeretek azonosítása és szétválasztása során lehet az adatcsomagokra épülő protokoll keret információit (vezérlő információk, sorszámok, hibajelző és hibajavító kódokat, időbélyegeket, IP, MAC címeket stb.) értelmezni, és felhasználni azokat a hálózati adatforgalom dekódolására.

A médiamenedzsment rétegbeli tevékenységek eredményeként állnak elő:

- 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 fogadott adatok.



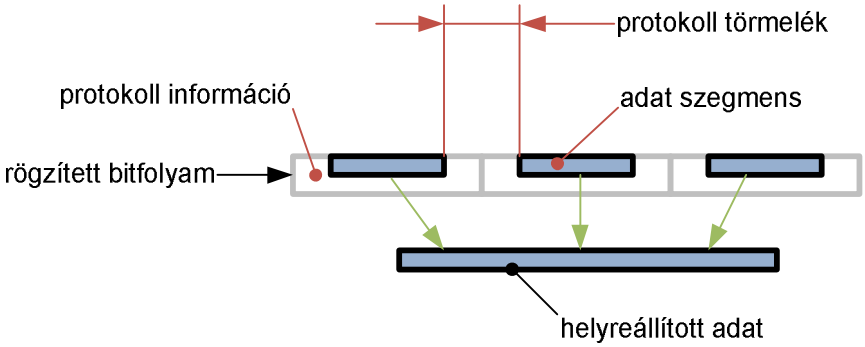
4. ábra – IP útválasztók sorozatát feltérképező `traceroute` parancs
ICMP csomagjainak folyamat diagramm részlete
[szerkesztette: Illési Zsolt]

Amennyiben a megjelenítési réteg vizsgálatakor a médiamenedzsment rétegből kinyert keretek magasabb szinten helytelen értelmezéshez vezetnek, úgy vissza kell térni az előző rétegben definiált feladatok elvégzéséhez valamilyen más megközelítést (például más protokoll bázist, más kezdőpontot) 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 adatvésési (data carving vagy file carving) technikát lehet alkalmazni a protokoll információk, vagy küldött/fogadott adatok helyreállítására. Az adatvésési technika az adatok struktúrája, belső adatai (metaadatok), az egyes protokoll információkra, adatformátumokra jellemző kódolási sajátosságok alapján kísérli meg a helyreállítást. Ez a megközelítés az adattárolókon a partíciós táblák, a fájlrendszer-leírók (például FAT tábla, vagy inode) sérülése esetén, vagy egyszerű szteganográfia alkalmazásának gyanúja esetén, fájltöredékekből való helyreállításhoz használhatók.

Jó példa erre a JPEG képek kódolása[1], ahol a fájl „`FF D8 … FF D9`" keretes szerkezetbe ágyazottak, ezek az értékek tetszőleges hexaeditorral kereshetők, így könnyen azonosíthatók és helyreállíthatók. A módszer következetes alkalmazásával az egymásba ágyazott képek is feltárhatók (például kép-indexkép reláció esetén).

A hálózati adatforgalom esetén a fenti technika 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:



5. ábra –Adatvésés hálózati adatfolyamból
[szerkesztette: Illési Zsolt]

A médiamenedzsment réteg egyik sajátos részterülete az azonosított adategységek (például fájlok) hitelességének, eredeti/ módosított/ hamis voltának vizsgálata. Kriptográfiai hitelesítő adatok hiányában ez információ és kódelméleti vizsgálatok 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 (a fájlok kiterjesztésének és a fájlok kódolásának összevetése), 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 infokommunikációs (hálózati), másodsorban információ és kódelméleti és informatikai felkészültséget igényel, de speciális hálózati alkalmazások adatforgalmának elemzéséhez szükség lehet programozói vagy az alkalmazás működésével kapcsolatos egyedi szaktudásra.

[1] Ld. ISO/IEC 10918-1:1994.

2.4 Alkalmazási réteg

Az alkalmazási réteggel kapcsolatos feladatok célja (a hálózati és protokollinformációktól megtisztított) adatok értelmezése, büntetőjogilag releváns információ kinyerése. Az alkalmazási rétegbeli vizsgálatok tárgya lehet informatikai jellegű, például az adatfájlok metaadatainak kinyerése, az adatokban található SQL, shell stb. parancsok értelmezése, programok visszafejtése, a kód-logika értelmezése a vizsgált cselekménnyel kapcsolatban.

Ebben a vizsgálati rétegben azonban már olyan egyéb – nem informatikai, telekommunikációs jellegű – adat is megjelenik, ami meghaladja az informatikai igazságügyi szakértő kompetenciáját. Fénykép esetén megállapítani a fényképen szereplő személy életkorát igazságügyi orvosszakértői feladat, szerzői védelem alá eső adatok (például program, kép, hang és videó fájlok) esetén az okozott anyagi hátrány megállapítása, vagy egyes esetekben a szerző, előadó azonosítása speciális (nem informatikai) szakértelmet és szakértői jogosítványokat kíván; így az ilyen adatokat tartalmazó ügyeket érdemben együttes, vagy egymást követő kirendelésekkel lehet szakszerűen lefednie a nyomozóhatóságoknak. (Például az informatikai igazságügyi szakértő feltárja a küldött-fogadott képeket, amelyeket ezután igazságügyi orvosszakértő elemez.)

Összefoglalás

Az infokommunikációs technológia átitatja a mindennapokat, meghatározó elemévé vált az üzleti életnek, a műszaki-tudományos világnak, de az egyének mindennapi életében is jelentős szerepet játszik. A technológia fejlődésével és terjedésével a „virtuális” megoldások egyre több teret nyernek a hagyományos megoldásokkal szemben. A levelet felváltotta az email és az SMS, a hagyományos vonalas telefonokat a mobil és az IP telefónia, a banki ügyintézők helyett (mellett?) terjed az eBanking… De a háttérben is nő az infokommunikáció szerepe. A kritikus – vagy jobban mondva a létfontosságú – infrastruktúrák is infokommunikáció segítségével csökkentik a működési költségeiket, növelik a hatékonyságukat és az eredményességüket.

Az infokommunikáció fejlődése nem csak a „fehér gazdaságra” igaz, hanem ugyanilyen (de legalább is hasonló) léptékben ismeri fel és használja ezt a technológiát a „szürke” és a „fekete” gazdaság is. És itt most nem csak a bűnözői csoportok kezében lévő hatalmas botnet hálózatokról, kiterjedt internetes pedofil képcserélő hálózatokról, a pénzügyi szektort támadó adathalász és hitelkártya-adat vadász csoportokra gondolok.

Számítógépet, internetet, mobil telefont használ(hat)nak a fehérgalléros bűnözők a bennfentes kereskedelmi tranzakció részleteinek egyeztetésére, a fekete galléros bűnözők egy rablás előkészítésre vagy lebonyolításakor, illetve a bűnös úton szerzett javak értékesítésére. De igazságügyi szakértői praxisomban találkoztam olyan esettel is, ahol a terhelt

- mobiltelefonja kamerájával vette fel a fiatalkorú partnerével eltöltött pásztoróra intim részleteit,
- házi eszközeivel szkennelt, editált és nyomtatott valódinak tűnő hamispénzt,
- egy rendőri túlkapásra hivatkozó leveléhez digitális felvételeket készített és szerkesztett a sérüléseiről.

Kimondható tehát, hogy a bűncselekmények széles körének vizsgálatakor az infokommunikációs eszközök büntetőjogilag releváns információkat (bizonyítékokat) hordoznak, így bizonyítékforrásként célszerű ennek a szektornak a kriminalsztikai, krimináltechnikai vizsgálatával foglalkozni. Szükség van e terület kutatására már csak azért is, mert az infokommunikáció naponta hoz újdonságokat – új protokollok, eszközök, kódolások stb. jelennek meg. Ezek elemzése, vagyis annak kutatása, hogy

- miképp használható az infokommunikációs technológia bizonyítékok kinyerésére,
- a technológiában rejlő adatok kinyerésének vannak-e, ha igen, akkor hol, törvényes akadályai,
- a „Ki?", „Mit?", „Hol?", „Mikor?", „Miért?", „Hogyan?" kérdésekre adnak-e és ha igen, akkor mennyire adekvát válaszokat

komoly fizikai, informatikai, telekommunikációs krimináltechnikai és kriminalisztikai, nyomozati probléma.

Ez az új – újszerű – terület új kutatási módszereket és technikákat igényel. A cikkben ennek a megközelítésére javaslok egy módszert, Brian Carrier réteg megközelítésének továbbgondolt verzióját, amely alkalmas a szakmai kompetenciák meghatározására és az együttműködés interfészeinek azonosítására. Véleményem szerint az általam javasolt megközelítés megkönnyíti a téma tudományos kutatását is.

Sajnos hazánkban ez a terület elhanyagolt. Nincs még olyan módszertani levél sem, ami a nyomozóhatóság nyomszerzési, nyomrögzítési tevékenységét és az ezt követő értékelő-elemző igazságügyi szakértői vizsgálatok általános szakmai szabályait, módszereit és technikáit rögzítené.

Véleményem szerint nagy szükség lenne egy ilyen módszertani levélre. Nem csak az igazságügyi szakértők, de a nyomozóhatóságok, sőt a jogászok (ügyészek, ügyvédek és bírák) is nagy hasznát vehetnék. Ugyanis a szakértő súlyos hibát követ el, ha nem a kirendelő határozatban megfogalmazott kérdésekre válaszol és úgy szolgáltat bármilyen bizonyítékot, hogy azt a kirendelő határozat nem kéri. {[10] p. 136.} Rossz, hiányos kérdésekre azonban csak rossz, hiányos válasz adható, a legnagyobb szakértői professzionalizmus mellett is elmaradhat a rögzített nyom szakszerű értékelése, így büntetőjogilag releváns tények maradhatnak „árnyékban" és a terhelt bűnösségének megállapításakor nem lehet figyelembe venni sem mentő, sem terhelő bizonyítékként.

A cikkben csak felületesen említettem egy olyan területet, amely szintén új kutatási feladatként kell, hogy megjelenjen a számítógépek krimináltechnikai vizsgálatában. Ez a kriptográfia. A magántitok, a bank és üzleti titok, a minősített adatok tárolása, továbbítása mellett a „rosszfiúk" is előszeretettel alkalmazzák ezt a jogellenes magatartásuk nyomainak elleplezésére. Amíg az általános kriptoanalízis teoretikusan közelíti meg a titkosítások megfejtésének kérdését, addig a bűnüldözőknek praktikus megoldások kellenek. A kérdés számukra az, hogy a terhelt által használt (pontosabban az általánosan is elterjedt és a leggyakrabban alkalmazott) kriptográfiai eszközöknek mi a gyengéje, hogyan férhetnek az elkövető titkaihoz, mivel és meddig érdemes próbálkozni, hogy korlátos idő- és pénzráfordítás mellett ésszerű határidőn belül eredményre lehessen jutni.

Remélem sikerült érzékeltetnem az információtechnológiai krimináltechnika előtt álló feladatokat és azok nehézségeit. A kutatások ezen a területen azonban önerőből, egy-egy szakértő önálló (sokszor egymástól elszigetelt) munkájával nem végezhető el. A tudományos alaposságú elemzéshez fejlesztéshez szükséges lenne szervezett kutatásra ami anyagi források nélkül elképzelhetetlen. Ehhez jelenleg azonban nincs olyan pályázat, vagy egyéb forrás, ami az igazságügyi szakértés kutatási, eszközpark bővítési problémáit megoldaná.

Egy a szakértői körökben forgó jogszabálytervezet a módszertani levelek elkészítését a Magyar Igazságügyi Szakértői Kamara feladatává tenné: „*30/A. § (1) A MISZK elnöksége (a továbbiakban: elnökség) a szakértői tevékenység egységes és magas színvonalú ellátása érdekében módszertani levelet ad ki*". A tervezet azonban nem rendel forrást a feladathoz – de nem ad ehhez „pénzt, paripát, fegyvert" egyéb más jogszabály tervezet sem. Tudomásom szerint módszertani levelek elkészítésébe kezdett a Nemzeti Nyomozó Iroda Csúcstechnológiai Bűnözés Elleni Osztálya, de az igazságügyi szakértői kamarától függetlenül…

Úgy gondolom, hogy az általam vizsgált kérdéskörnek a koordinálását és

menedzselését az Igazságügyi és Rendészeti Minisztériumnak kellene felvállalnia, kutatóhelyek teremtésével és pályázatok kiírásával együtt. Így ez a most elhanyagolt terület fejlődésnek indulhatna és a krimináltechnikai vizsgálatok is megfelelnének a kor társadalmi-tudományos elvárásainak.

Irodalomjegyzék

[1] 1998. évi XIX. törvény a büntetőeljárásról (Be.)

[2] Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998.

[3] Brian Carrier: Defining Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence, 2003. Volume 1 Issue 4., Economic Crime Institute (ECI) at Utica College, USA, 2003.

[4] Eoghan Casey: Digital Evidence and Computer Crime – Forensics Science, Computers and the Internet, 2nd edition, Elsevier Academic Press, California, USA, 2004.

[5] Illési Zsolt: Krimináltechnika Szerepe az Informatikai Védelem Területén, Hadmérnök, IV. Évfolyam 1. szám - 2009. március, Budapest, 2009. [IZs2]

[6] Illési Zsolt: Open Source IT Forensics, avagy Nyílt Forráskódú Programok Felhasználása az Informatikai Igazságügyi Szakértésben, Bolyai Szemle 2008. XVII. évf. 4. szám, ZMNE Bolyai János Katonai Műszaki Kar, Budapest 2008. [IZs1]

[7] Linda Volonino PhD, Reynaldo Anzaldua: Computer Forensics for Dummies, Wiley Publishing, Inc., Indianapolis, USA, 2008.

[8] Szerk.: Dr. Bócz Endre: Kriminalisztika, BM Kiadó, Budapest, 2004.

[9] Szádeczky Tamás: Terrorizmus a kibertérben, Infokommunikáció és jog, 2008. V. évf. 6. sz. pp. 200-205.

[10] Tremmel Flórián: Bizonyítékok a büntetőeljárásban, Dialóg Campus, Budapest-Pécs, 2006.

[11] Vayne Jansen, Rick Ayers: Guidelines on Cell Phone Forensics (NIST 800-101), National Institute of Standards and Technology, USA, 2007.

[12] http://hu.wikipedia.org/wiki/Számítógép-hálózat