HADMÉRNÖK

IV. Évfolyam 3. szám - 2009. szeptember

Illési Zsolt
illesi.zsolt@proteus.hu

WIFI HÁLÓZATOK IGAZSÁGÜGYI SZAKÉRTŐI ELEMZÉSE: WIFI HÁLÓZATOK FELDERÍTÉSE

Absztrakt

Az informatikai rendszerek komplexitása miatt nem csak az elkövetők kerülhetnek a nyomozóhatóság látókörébe, hanem ártatlan személyek is, hiszen az informatikai bűncselekmény elemei lehetnek olyan wifi végpontok, amelyeket a bűnelkövetők „hekkeltek" meg és használták fel. Mivel hatóság a wifi végpontokkal kapcsolatos bűnügyekben nyomozhat mind bűnös, mind bűntelen terheltek után, ezért lényeges kérdés, hogy a nyomozás során valamennyi terhelő és a terheltet mentő bizonyítékot összegyűjtsön. Cikkben egy olyam módszer kerül bemutatásra, amely alkalmas lehet a wifi hálózatok felderítésére, az ügyben érintett wifi végpontok azonosítására, a releváns technikai adatok összegyűjtésére, elemzésére és vizuális megjelenítésére.

Because of the complexity of the information systems not only the wrongdoers can get into the sight of the investigating authorities, but innocent persons since it is possible that one element of a crime is such a wifi stations that were hacked and used by offenders. Since authorities may make investigations on wifi stations for both guilty and innocent accused, it is an important question to collect all relevant incriminating and exculpating evidence during the examination. In this article a method for wifi network reconnaissance is presented which is suitable for collecting, analysing and visually presenting relevant technical data for all wifi components that may be concerned in the case.

Kulcsszavak: *informatikai védelem, kriminalisztika, krimináltechnika, digitális nyom, nyomozás, wifi hálózatok felderítése, térinformatika ~ information security, forensic science, applied forensics, digital trace, investigation, wifi network detection, geographic information system, GIS*

Bevezetés

Az informatikai rendszerek elterjedésével nő az azokkal kapcsolatos bűnözés mértéke. Kriminológiai szempontból egy informatikai rendszer (annak hardver, szoftver komponensei, kommunikációs hálózata vagy annak szegmensei) 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 informatikai 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 informatikai rendszer vagy eszköz, de a bűncselekmény során a terhelt valamilyen hardver, szoftver eszközre vagy kommunikációs hálózatra hivatkozva vezeti félre a sértettet (pl. olyan a 1978. évi IV. törvény a Büntető Törvénykönyvről (a továbbiakban Btk.) 318. § szerint csalásnak minősülő eset, ahol az elkövető nem létező számítógépeket ad el a sértettnek);
- ***elkövetés „tanúja”***, ha a bűncselekménnyel összefüggésben lévő bizonyítékként felhasználható releváns adatot rögzít egy informatikai eszköz (pl. az internet szolgáltató hálózati eszközei naplózzák egy a Btk. 261. § szerinti terrorcselekmény valamely lényeges körülményét, vagy elektronikus hang és/vagy képfelvétel készül egy a Btk. 197. § szerinti erőszakos közösülésről, vagy az elkövetők elektronikus levelezés során terveznek meg egy a Btk. 166. § szerinti emberölést és a postaláda megőrzi a levélváltást) függetlenül attól, hogy az tettes célja egy informatikai rendszer valamely komponense volt-e vagy sem, használt-e informatikai eszközt az elkövetéshez vagy sem.

[3][1][7]

Informatikai rendszereket használnak egyszerű, mindennapi emberek a mindennapi céljaikhoz, ilyen eszközökkel növelve a komfortot, a munkájuk hatékonyságát, a mobilitásukat. A „normál” felhasználók mellett a bűnözők is használják az információs technológiát ugyan olyan okokból, mint mindenki más, de a technológia lehetővé teszi számokra a bűnelkövetés hatékonyságának és eredményességének növelését, valamint segít a nyomaik eltüntetésében.

Az informatikai rendszerek komplexitása miatt nem csak az elkövetők kerülhetnek a nyomozóhatóság látókörébe hanem ártatlan, de egy informatikai rendszer – informatikához, információbiztonsághoz hozzá nem értő – tulajdonosai, üzemeltetői is, hiszen az elkövetés valamelyik tárgya, vagy az informatikai bűncselekmény (virtuális) helyszínének lehetnek elemei olyan számítógépek, amelyeket a bűnelkövetők „hekkeltek” meg, használták fel.

A rendőrség (vagy ügyészség) a vizsgálatai során tehát nyomozhat mind bűnös, mind büntelen terheltek után, ezért lényeges kérdés, hogy az üggyel kapcsolatos valamennyi releváns tényt, adatot összegyűjtsön. A nyomozást végzők feladata azonban nem csak a koncepcióikat alátámasztó, csak a vádhatóság igényeit kiszolgáló terhelő bizonyítékok, hanem a terheltet mentő bizonyítékok feltárása, hogy lehetőleg ártatlan emberek ellen ne induljon büntetőeljárás, vagy ha indult, akkor mihamarabb felfüggesszék az ilyen cselekményeket.

Jelen dolgozatomban a wifi hálózatok (IEEE 802.11 /a, /b, /g, /n) felderítésével kapcsolatos, a releváns tények feltárását segítő, nyomozati, szakértői cselekményeket szeretném meghatározni, a mérési, értékelési módszereket feltárni, illetve rávilágítani a wifi hálózatok felderíté-

séből származó adatok büntetőeljárásban való bizonyítékként felhasználhatóságának korlátaira.

Wifi hálózatok

A wifi hálózatok főbb jellemzői

Az IEEE 802.11 által definiált mikrohullámú helyi (LAN vagy P2P) hálózati protokoll családot összefoglaló néven wifi hálózatoknak nevezzük. A wifi hálózatok előnye, hogy nincs szükség közvetlen vezetékes kapcsolatra a számítógépek közti kommunikáció során, hanem az állomások DSSS modulációjú[1] mikrohullámú rádióhullámok segítségével kommunikálnak egymással. A protokoll család jellemzően CSMA/CA[2] protokollt használ az adatcserére.

A wifi csomagok azonos szerkezetűek, melyet a szabvány az alábbiak szerint határoz meg:

2 bájt	2 bájt	6 bájt	6 bájt	6 bájt	2 bájt	6 bájt	0- 2312	4bájt
Frame Control	Duration	Address 1	Address 2	Address 3	Seq	Address 4	Data	Check sum

1. ábra. A 802.11/x protokoll család MAC keretformátuma
(forrás: [8] p220)

A állomások wifi antennái rendszerint egyszerű bot antennák, vagyis olyan monopol antennák amelyek karakterisztikája közelítően nem szimmetrikus torroid alakú, amit a környezet (főleg az épületek, nagy fém tárgyak) jelentősen képesek befolyásolni. Az általános karakterisztikájú antennák mellett azonban lehet vásárolni irányított karakterisztikájú antennákat is (pl. SMC smchmant-6-eu), illetve a wifi hekkerek előszeretettel javítják fel a gyári eszközöket és alakítanak ki irányított karakterisztikájú antennákat, amelyek jellemzői jelentősen eltérnek a „gyári” értékektől.

Az antenna karakterisztika módosításához még híradónak vagy profi villamosmérnöknek sem kell lenni, hiszen a tuningoláshoz az interneten rengeteg tippet és trükköt lehet találni például a youtube-on[3], vagy akár a hazai nyomtatott sajtóban – például a Chip Magazinban[4] – is egyszerűen kivitelezhető tanácsok találhatók.

---

[1] DSSS – Direct Sequential Spread Spectrum (közvetlen sorrendes szórt spektrumú) kódoláskor az adatfolyam, az átviteli sávszélességnél nagyobb sebességű digitális kóddal szorozódik össze. Minden adatbit az adó- és a vevőállomás által ismert álvéletlen (ú.n. chip kód) sorozattal szorozódik össze. Dekódoláskor az ismert chip kódot összeszorozva a kódolt jellel invertálva „0”-t kapunk, nem invertálva pedig az adatfolyam „1” értékét kapjuk.

[2] CSMA/CA – Carrier Sensing Multiple Access/ Collision Avoidance (ütközést elkerülő, vivőérzékeléses többszörös hozzáférés) rádióhálózatokban használható protokoll, amelyben a kommunikációban résztvevő állomások a többi állomás adását figyelve figyelik a csatornát. Az aktív adás befejezése után minden állomás egy adott ideig vár – ezt az időt egy, a protokoll által meghatározott logikai listában elfoglalt helyük határoz meg. Ha ez alatt az idő alatt más állomás nem kezd adni, akkor az adásra várakozó állomás elkezdi a kommunikációt.
Vezetékes hálózatokban inkább elterjedt a CSMA/CD – Carrier Sense Multiple Access with Collision Detection (ütközést jelző vivőérzékeléses többszörös hozzáférés) protokoll, amelynél az adást kezdeményezni kívánó adó a kommunikáció megkezdése előtt belehallgat a csatornába, és csak akkor küldi el az üzenetét, ha a csatornát más nem használja. Az adó az adás közben folyamatosan veszi saját jelét – összehasonlítva a kimenő és a bejövő jeleket érzékeli, ha más vele versengő adó vele együtt ad (érzékeli az ütközést); ekkor felfüggeszti az adást és véletlenszerű ideig vár, majd újra kezdi az adást.

[3] Ld.: http://www.youtube.com/watch?v=QmF2iiEt4kU

[4] WiFi antenna házilag, Takarítson meg több ezer forintot, javítsa hálózati sebességét a CHIP antennájával! in CHIP Magazin 2009/3, p 60-61, Infopress Group Hungary Zrt., Budapest, 2009.

Az adatátvitel maximális sebességét a protokoll rögzíti, ez azonban a mikrohullámú rádiós kommunikáció sajátosságai miatt egyéb tényezőktől is függ. Ilyen tényező lehet:

- környezetben lévő tereptárgyak;
- környezeti és időjárási viszonyok;
- elektromágneses zavarok.

[8][11]

A wifi hálózatok jellemző paramétereinek összefoglalása az alábbi táblázatban található:

IEEE szabvány	Működési frekvencia [GHz]	Jellemző sebesség [Mbit/s]	Maximális sebesség [Mbit/s]	Hatótávolság beltérben [m]	Hatótávolság kültérben [m]
802.11a	5	23	54	~35	~120
802.11b	2,4	4,3	11	~38	~140
802.11g	2,4	19	54	~38	~140
802.11n	2,4 / 5	74	248	~70	~250

1. táblázat. Wifi hálózatok főbb paramétereinek összehasonlítása
(forrás: [11])

A wifi hálózat főbb komponensei:

- hozzáférési pont (Wireless Access Point, WAP vagy AP) amely egy olyan kommunikációs eszközt jelent, amely mások számára elérhetővé teszi a wifi hálózat használatát, ezek rendszerint a wifi és a kábeles hálózatot összekötő útválasztók;
- wifi berendezések, olyan eszközök, amelyek képesek a wifi hálózaton keresztül kommunikálni.

Wifi hálózat létrejöhet:

- hozzáférési pont(ok) között;
- hozzáférési pont és wifi berendezés(ek) között;
- wifi berendezések között közvetlenül (ezek az ún. ad-hoc hálózatok).

A wifi hálózat lehet:

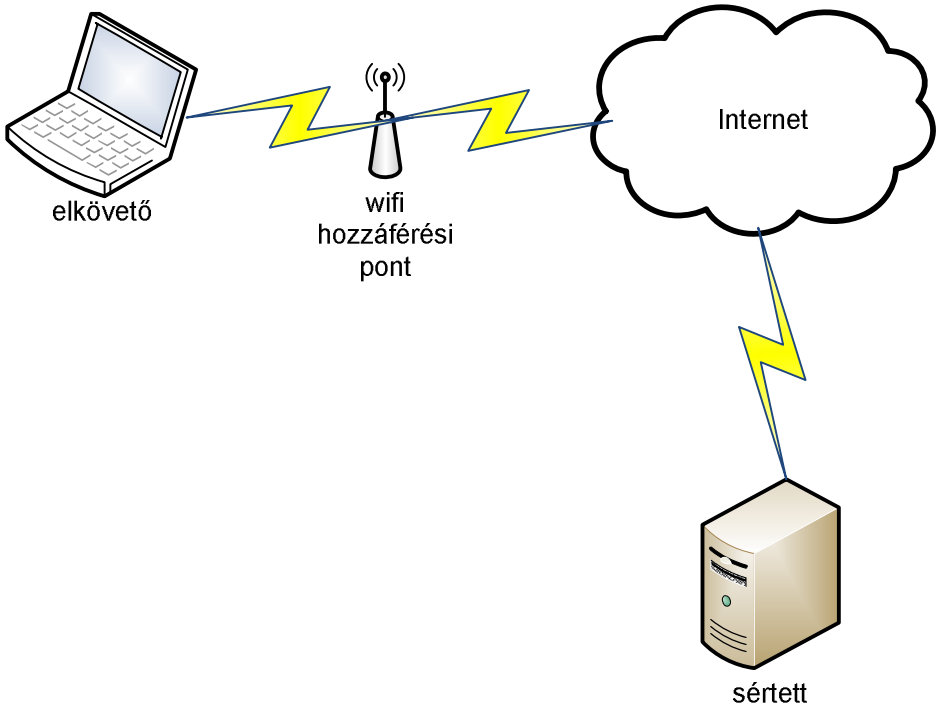
- védetlen (titkosítással nem védett);
- gyengén védett (Wired Equivalent Privacy – WEP kódolással védett);
- védett (Wifi Protected Access – WPA vagy WPA 2 titkosítással védett).

Wifi hálózatok az informatikai bűncselekményben

Amennyiben egy wifi hálózat része egy informatikai, vagy az informatikával összefüggő bűncselekmény valódi vagy virtuális helyszínének, vizsgálni kell, hogy:

- Hogyan lehet egy wifi hálózathoz kapcsolódni?
- Honnan lehet a wifi hálózathoz kapcsolódni?
- Milyen bizonyíték értéke van a wifi hálózatból szerzett információnak?

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



2. ábra. Wifi hálózatot is érintő bűncselekmény elvi vázlata
(szerk.: Illési Zsolt)

Ilyenkor a kommunikáció során a résztvevő informatikai 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 probléma az, hogy a MAC cím csak a következő útválasztóig azonosítja a számítógépet, ez után az adatot továbbító útválasztó MAC címe azonosítja a csomagot a következő útválasztóig. A MAC címet egy közepesen képzett informatikában alig járatlan felhasználó is képes megváltoztatni megfelelő segédprogramok segítségével, amelyekből jó néhány található meg egy gyors Google-es 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 azonban előfordulhat, hogy a forrás számítógép MAC címe túlél egy-egy kommunikációs csomópont közi ugrást (pl. a MS Word által készítet dokumentumokban tárolt egyedi azonosítókban) így felhasználható az azonosításra.

A forrás IP címe már egy kicsit több információval szolgáltat, 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.

Az UDP alapú kommunikációnál – ha a elkövető csak egy irányban használja a csatornát – szintén nem használható fel a kommunikációban szereplő IP címe.

Az IP címek felhasználhatóságának korláta még az esetleges virtuális magáncsatornák alkalmazása, amikor a elkövető egy titkosított csatornán át, esetleg több számítógépen keresztül éri el a sértett számítógépét. Ilyen esetben csak a titkosított csatorna két szélén lévő határ titkosító 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 jegyeznem, hogy a wifi 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 elkötésre 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.).

A wifi hálózatok esetén lényeges szempont továbbá az, hogy egy-egy csomag csak milliszekundumokig „él" és a hálózat által lefedett területen fogható.

A vezeték nélküli hálózatokhoz kapcsolódó végpontok térereje azonban a kapcsolat ideje alatt végig mérhető, így adatot szolgáltat arról, hogy a kommunikáció során mely más végpontokkal kommunikálhat.

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

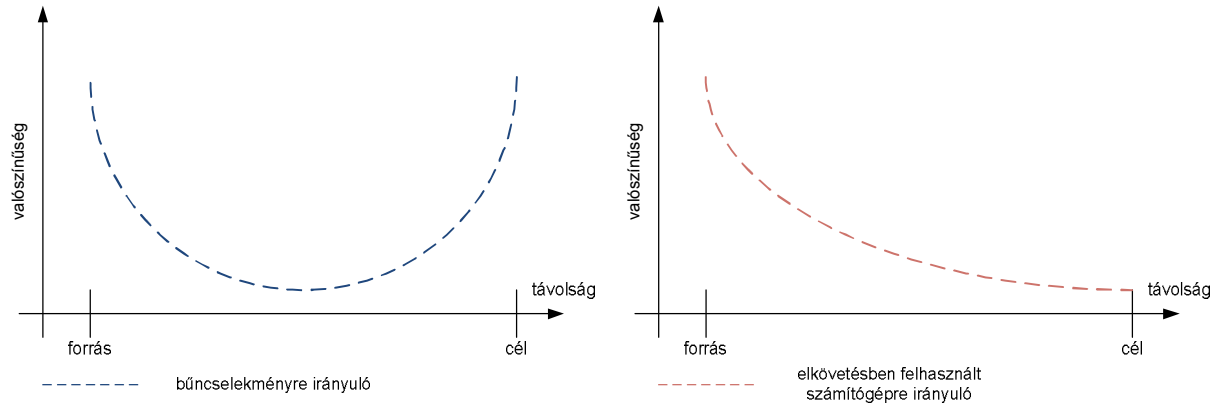
- a forrás számítógép;
- a sértett számítógépe (cél);
- a kommunikációban résztvevő valamennyi informatikai eszköz (így a wifi végpont)

a memóriájában, naplóállományokban stb.

A fentiekből következik tehát, hogy a wifi hálózat elemzéséből kinyerhető bizonyítékok:

- bizonyító ereje (az esemény valószínűségét megerősítő volta) és
- a típusa, vagyis
  - az elkövetésben felhasznált számítógép – „személyi vonatkozású", vagyis az elkövetéshez felhasznált eszközzel kapcsolatos gyanút növelő tényező, vagy
  - az elkövetett cselekményre – tárgyi vonatkozású, a bűncselekményre irányuló, azzal kapcsolatos gyanút növelő tényező

összefüggésben van az adatszerzésnek a forrástól vagy a céltól való távolságával. Ezt a kapcsolatot az alábbi ábra szemlélteti:



3. ábra. Wifi hálózatból kinyerhető bizonyítékok bizonyító ereje, típusa a forrástól és a céltól való távolság függvényében (szerk.: Illési Zsolt)

A nyílt hálózatokhoz bárki csatlakozhat – egyes esetekben akár véletlenül is – tehát az ilyen hálózatokhoz kapcsolódó vizsgálatok esetén mindig vélelmezni kell, hogy a hálózati forgalmat nem csak a jogosult felhasználók generálták, bárki kívülről is lehetett az adó/vevő.

A gyakorlatban a WEP kódolású hálózat védelme 1 perc alatt törhető; a wifi hálózat kódoláshoz nem kapcsolódó egyéb védelmi mechanizmusai, mint a MAC cím szűrés, a hálózati azonosító (SID) sugárzásának tiltása hatástalan. A SID-et a hálózati forgalom lehallgatásával meg lehet ismerni (ez minden csomagban nyílt formában megtalálható), a MAC cím pedig klónozással egyszerűen megváltoztatható a hálózatban aktívan kommunikáló számítógépek MAC címeinek ismeretében gyorsan és hatékonyan. Ezek alapján kijelenthető, hogy a WEP kódolással védett wifi hálózatok viszonylag alacsony informatikai felkészültségű elkövető számára is eredményesen támadhatók, ezért vélelmezni lehet, hogy az ilyen hálózatokba nem csak a hálózat rendszergazdája/üzemeltetője által engedélyezett felhasználók kapcsolódhatnak.

A WPA és a WPA2-es hálózatokat biztonságosnak lehet mondani, amennyiben az alkalmazott kulcsméret elegendően nagy (nagyobb, mint 16 karakter) és az alkalmazott kulcs entrópiája (az alkalmazott jelkészlet véletlenszerűsége) 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 védetlen;
- 31%-a WEP kódolású;
- 27%-a WPA vagy WPA2 titkosítással védett.

[9]

Ezekből az adatokból egyértelműen kiviláglik, hogy amennyiben egy bűncselekmény elkövetése során wifi hálózati elem is része a bűncselekmény fizikai vagy virtuális helyszínének úgy a végpont karakterisztikája, az alkalmazott kódolás típusa az ügy szempontjából releváns, és ezeket a jellemzőket a nyomozás során érdemben vizsgálni kell.

Wifi hálózatok felderítésével kapcsolatos nyomozati cselekmények

Helyszínhez (is) kapcsolódó nyomozási cselekmények általában

Kriminalisztikai szempontból „*helyszínen értjük azt a helyet a hol a feltételezett bűncselekményt elkövették avagy a bűncselekmény részét alkotó vagy azzal összefüggő egyéb részcselekmény, esemény stb. lezajlott*”. ([10] p 174)

A fenti definíció alapján az informatikai bűncselekmények helyszíne – így a wifi hálózatot is magában foglaló helyszín – többes, sok lehetséges fizikai és virtuális helyszín együttesen alkothatja az elkövetés teljes színterét. Az informatikai bűncselekmény helyszíne magába foglalja az elkövetőt, a megtámadott számítógépét, a támadási útvonalba eső internet szolgáltatók kommunikációs eszközeit, valamint a támadás során használt számítógépeket, egyéb infokommunikációs eszközöket, valamint ezek logikai és fizikai környezetét.

A nyomozás során a helyszínhez a következő cselekmények kötődnek:

- ***helyszíni szemle*** – olyan nyomozási cselekmény amely 1998. évi XIX. törvény a büntetőeljárásról (a továbbiakban 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.

[2]

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

	HELYSZÍNI SZEMLE	**BIZONYÍTÁSI KÍSÉRLET**	**HELYSZÍNELÉS**	**FELISMERÉSRE BEMUTATÁS**
(Tipikusan) halaszthatatlan 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 (ld. hallás-próba → ingerküszöb, hallhatóság)	emlékezeti választás	emlékezeti választás (ld. beszédfelismerés, hangkiválasztás)

2. táblázat. A helyszíni szemle és a helyszínhez (is) kapcsolható nyomozási cselekmények elhatárolásának összefoglalása (forrás: [10] 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
  - 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 (bűncselekményre irányuló gyanú és esetleg elkövetői gyanú is fennáll, de a bűncselekményt megvalósító cselekménynek az oka ismeretlen) cselekményekkel kapcsolatosak.

[10]

Wifi hálózatok felderítésével kapcsolatos speciális nyomozati cselekmények

A wifi hálózatok felderítésével kapcsolatban a következő nyomozási cselekmények hajthatók végre:

- helyszíni szemle (annak vizsgálata, hogy a szemle idején milyen a wifi hálózat karakterisztikája, milyen állomások érhetők el a fizikai helyszínről, milyen kódolás van beállítva);
- bizonyítási kísérlet (annak vizsgálata, hogy valamely időben el lehetett-e érni a vezeték nélküli hálózati elemet, a kérdéses eszköz milyen távolságban, milyen technikai paraméterek mellett működő eszközzel kommunikálhatott, illetve milyen eszközökkel nem.);
- helyszínelés (amely során a terhelt vagy tanú a hálózat valamely lényeges paraméterével, működési módjával vagy körülményével kapcsolatos tényt, adatot, vagy tárgyi bizonyítékot szolgáltat).

A nyomozási cselekményekről általánosan kimondottak alapján kimondható, hogy a wifi hálózatokkal kapcsolatos speciális nyomozati cselekmények típusa vagy a nyomozási tervtípus függvényében általában lehet:

- titkos vagy nyílt;
- halaszthatatlan vagy normál;
- ismeretlen tetteses, ismert tetteses vagy ismeretlen okú.

A vezeték nélküli hálózatoknál leírtak alapján azonban – figyelembe véve az adatok rövid élettartamát és az ügy szakértői értékelésére, ezáltal a megítélésére gyakorolt hatásait– a hálózat helyzetével és karakterisztikájának felderítésével kapcsolatos nyomozási cselekmények elsősorban halaszthatatlan cselekmények – különösen a helyszíni szemle, függetlenül a tettes vagy az ok ismertségétől és ezek a cselekmények egyaránt végezhetők nyílt és titkos formában.

Másodsorban a vezeték nélküli hálózatok felderítésével kapcsolatban – amennyiben a helyszíni szemle elmaradt, vagy hiányos volt – szóba jöhet még a bizonyítási kísérlet vagy a helyszínelés is.

Wifi hálózatok felderítésének módja

A vezeték nélküli hálózatok felderítéséhez szükséges

- hardver eszközök:
  - hordozható számítógép,
  - wifi,
  - GPS,
- szoftver eszközök:
  - wifi hálózatfigyelő szoftver,
  - térinformatikai alkalmazás.

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

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

- helyre vonatkozó (mi található egy adott helyen);
- körülményekre vonatkozó (hol van a keresett objektum, tereptárgy vagy eszköz);
- trendekre vonatkozó (mi változott meg, illetve a változások milyen jellegzetességet mutatnak);
- útvonalra vonatkozó (melyik a legkedvezőbb út egy pontból egy másikba);
- jelenségre vonatkozó (mi a jelenség, illetve mik a jelenséget meghatározó legfontosabb tényezők);
- modellezési (mi történik, ha a környezet valamely paramétere megváltozik);

kérdésekkel kapcsolatban, és az elemzések adatait vizuális formában (jelek, grafikus ábrák, képek stb.) megjeleníteni. [[4] p. 25]

Az így kapott vizuális elemzések már alkalmasak a szakértői megállapítások demonstrálására az informatikában nem járatosak számára is.

Az igazságügyi szakértők számára sajnos azonban ilyen, általános célú, térinformatikai eszköz nem áll rendelkezésre, ezért a demonstráció során a hálózatokkal kapcsolatos technika és térbeli adatainak kinyerésére a Network Stumbler-t, az adatok elemzésére és a vizuális megjelenítés előkészítésére a Pearl és Pearl GD modult felhasználó Footprint alkalmazást, a földrajzi megjelenítésre Google Earth-t használtam, mivel ezek együttesen alkalmasak a wifi hálózatok felderítésének minimális vizsgálatára.

Egy professzionális GIS szoftverrel azonban az elemzési lehetőségek sokkal széles körűbbek lehetnének, például figyelembe lehetne venni a terepviszonyok vagy az épületek hatását.

A rendszer másik „kritikus” pontja a wifi kártya, ennek a meghajtó programjának 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. 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.

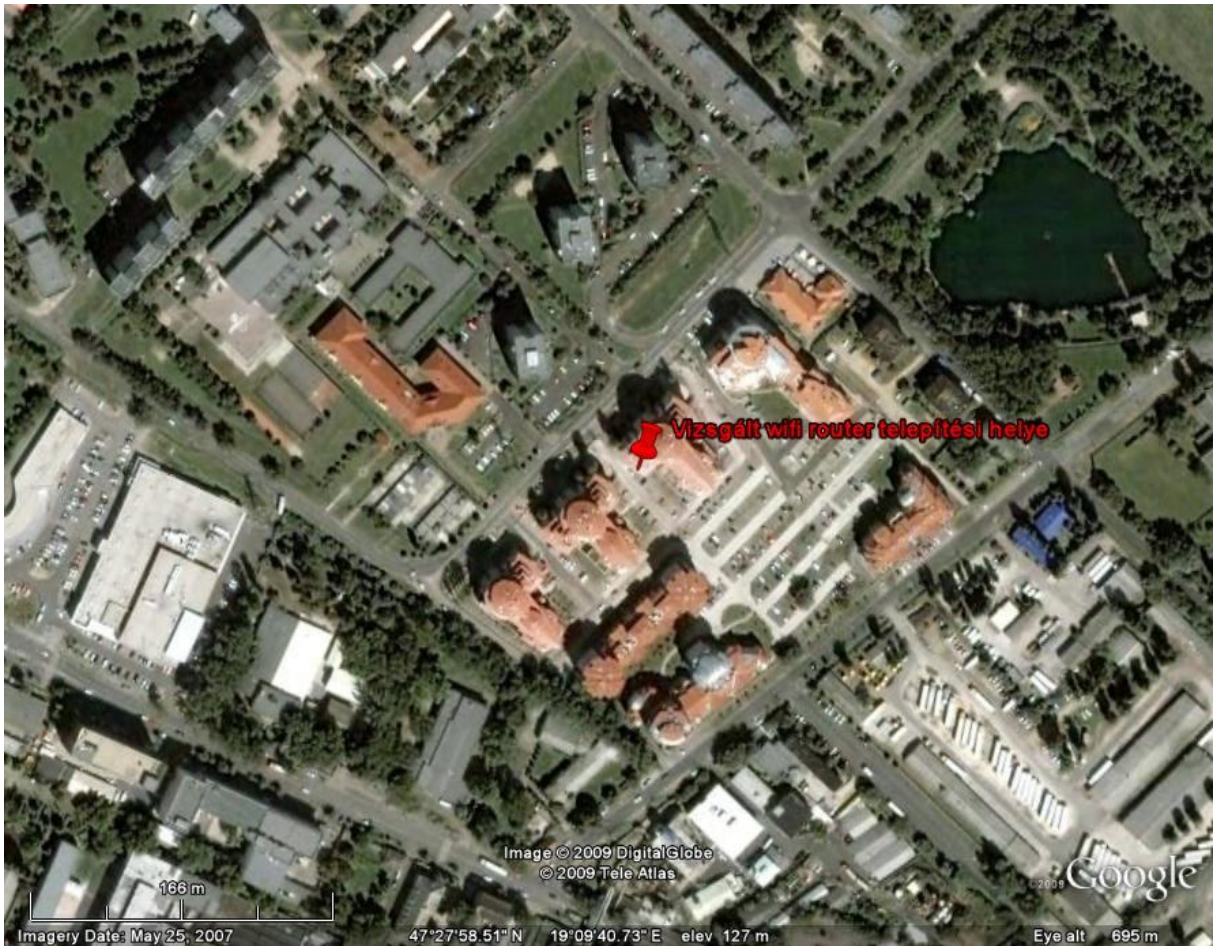
A továbbiakban bemutatott ábrák, adatvédelmi megfontolások miatt – mivel a cikkem célja csak a vezeték nélküli hálózatok felderítésének a krimináltechnikában is alkalmazható módszerének demonstrációja – a helyszínek, hálózati azonosítók nem felelnek meg egy valós helyszín adatainak sem, a mérési adatokat a publikáció előtt módosítottam.

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.

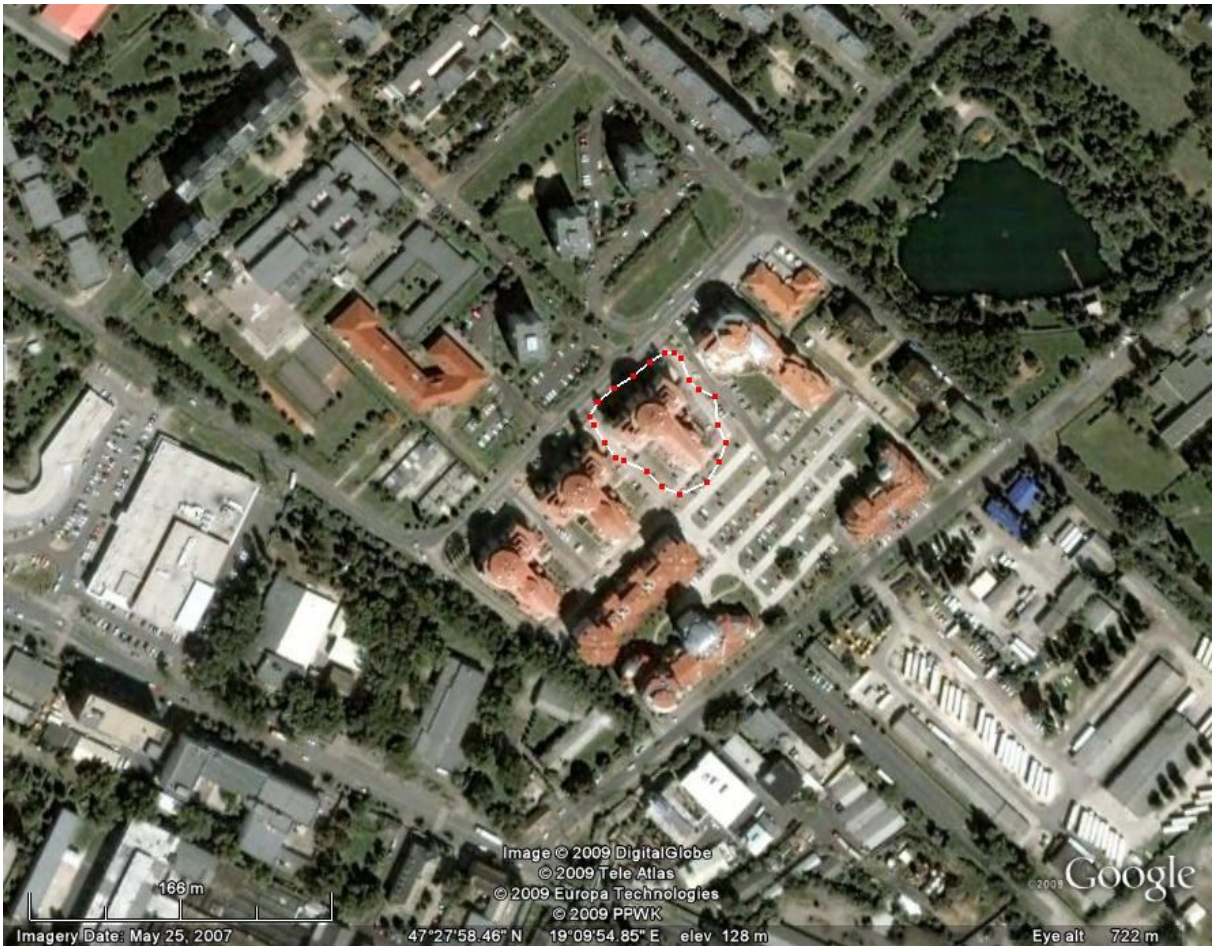
1) Adatgyűjtés

A nyomozás kezdeti szakaszában először valószínűleg az elkövetés során használt wifi végpont IP címét, illetve az ezt üzemeltető személy (vagy szervezet) címét sikerül megszerezni. Ezt a címet a Google Earth program segítségével viszonylag könnyen lehet ábrázolni a helyazonosító (placemark) térképre illesztésével. Ez történhet a hely pontos földrajzi koordinátáinak beírásával, de megadható manuálisan is.



4. ábra. Feltételezett helyszínen a wizsgált router telepítési helye
Google Earthben ábrázolva (forrás: Illési Zsolt)

A helyszín azonosítását követően az aktív GPS és wifi modulal felszerelt mobil eszközzel körbe kell járni a célterületet – nagyobb terület esetén spirálisan, hogy felmérjük az észlelhető hálózatokat.



5. ábra. A wifi hálózat feltérképezése során a mobil mérőegységgel bejárt útvonal Google Earthben ábrázolva (forrás: Illési Zsolt)

A Network Stumbler által rögzített információk a következők:

- MAC (Media Access Control): a hálózati eszköz azonosítására alkalmas 12 bájtos fizikai címe (00-13-F7-39-82-B9), amelynek az első 6 bájtja a gyártót (a példa esetében ez a SMC Networks, Inc.), az utolsó hat bájt pedig az eszközhöz köthető egyedi azonosító;
- SSID (Service Set Identifier): a vezeték nélküli hálózat maximum 32 betűből és számból álló azonosítója, amely nem egyedi, sőt – ha a felhasználó nem módosítja – a gyártó által beállított érték is lehet (ez az érték lehet üres is, amennyiben az állomás által forgalmazott csomagok ezt nem tartalmazzák.);
- Name: az eszköz neve (ez csak abban az esetben jelenik meg, ha az eszközben a „Query APs for names” be van állítva);
- Chan(nel): a 802-es szabvány lehetővé teszi, hogy az adók a rendelkezésre álló frekvenciatartománynak csak egy szeletét használják ki, ezáltal elkerülhető, hogy az egymás mellé telepített hálózatok zavarják egymást. A rendelkezésre álló csatornák 1-11-ig;
- Speed: a hálózati végpont sebessége;

- Vendor: az eszköz hálózati kártyájának gyártója (a MAC cím alapján);
- Type: az eszköz típusa,ami lehet „AP” vagy „Peer” attól függően, hogy infrastrukturális vagy végfelhasználói eszközről van-e szó;
- Encryption: az alkalmazott titkosítás (semmi/ WEP/ WPA vagy WPA 2);
- SNR (signal-to-noise ratio): a jel zaj arány;
- Signal +: a legerősebb mért hasznos jel;
- Noise-: a legerősebb mért zaj;
- SNR+: a legmagasabb mért SNR érték;
- IP addr(ess): az eszköz IP címe(i);
- Subnet: az eszköz alhálózata (amelyek rendszerint A, B vagy C osztályúak lehetnek);
- Latitude: földrajzi szélesség[5];
- Lognitude: földrajzi hosszúság[4];
- Distance: távolság[4];
- First Seen: az eszköz érzékelésének első időpontja;
- Last Seen: az eszköz érzékelésének utolsó időpontja;
- Signal: az aktuális jelerősség;
- Noise: az aktuális zajerősség;
- Flags: a vezeték nélküli hálózat működését leíró „capability” értékek[6] hexadecimálisan;
- Beacon Interval: a csomagok közti szünet. [6]

2) A hálózat térerejének karakterisztikáját jelző „hőtérkép” elkészítése

Az adatgyűjtést követően a Network Stumbler által mért adatokat kiexportálva a Footprint elkészíti az összes észlelt vezeték nélküli hálózat karakterisztikáját „hőtérkép” formájában, amihez kapcsolja a jel földrajzi koordinátáit is. [8]

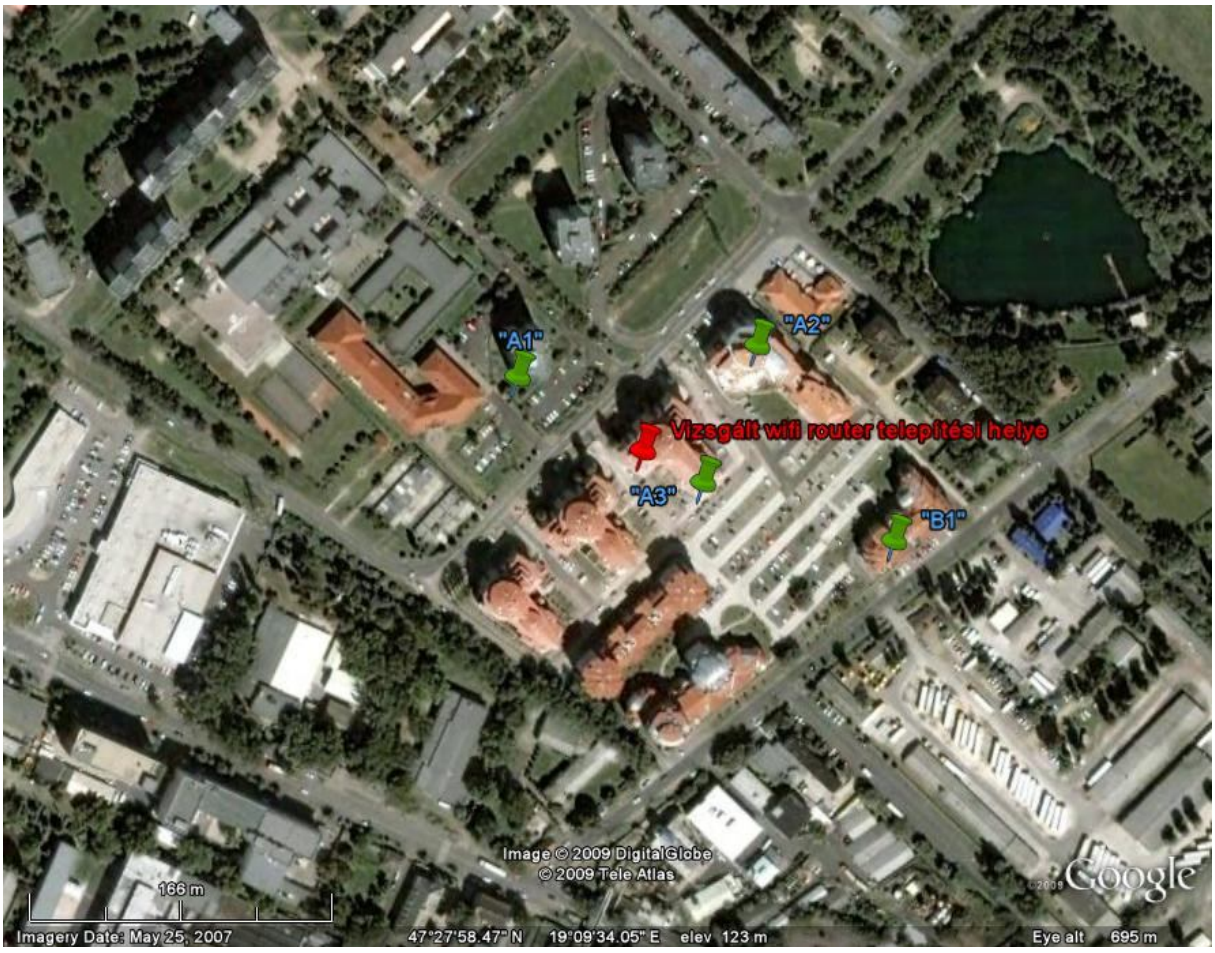
[5] A szélesség, hosszúság és távolság értékeket a rendszer a jelerősség alapján becsüli.

[6] A capability flag lehetséges értékei a netstumbler súgója alapján a következők lehetnek: [6]

Flag		Jelentés	Meghatározó szabvány
Decimális	Hexadecimális		
1	1	ESS	802.11
2	2	IBSS	802.11
4	4	CF Pollable	802.11
8	8	CF-Poll Request	802.11
16	10	Privacy (WEP)	802.11
32	20	Short Preamble	802.11b
64	40	PBCC	802.11b
128	80	Channel Agility	802.11b
1024	400	Short Slot Time	802.11g
8192	2000	DSSS-OFDM	802.11g
256, 512, 2048, 4096, 16384, 32768	100, 200, 800, 1000, 4000, 8000	Reserved for future use.	802.11g

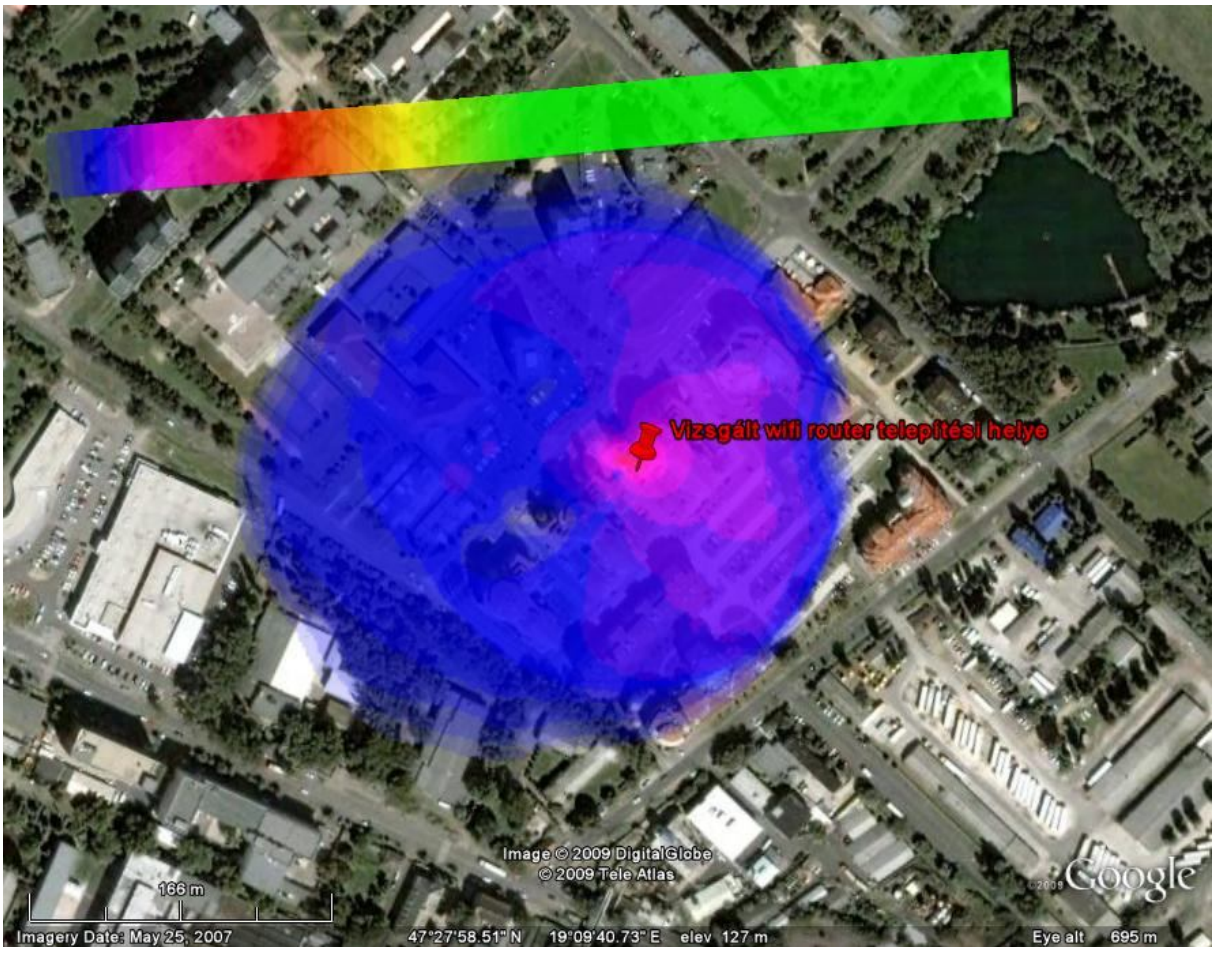
3) A gyűjtött adatok térképen való megjelenítése

Az adatgyűjtést követően a Network Stumbler által becsült földrajzi koordináták és távolság segítségével első körben a Google Earth-re fel lehet tenni egyedi objektumként az összes észlelt vezeték nélküli hálózati eszközt a vizsgált wifi eszköz telepítési helyénél leírtaknak megfelelően:



6. ábra. A vizsgált router környezetében érzékelt wifi végpontok
Google Earthben ábrázolva (forrás: Illési Zsolt)

Az eszközök feltételét követően a vizsgált eszköz karakterisztikáját bemutató „hőtérképet” is fel lehet tenni a Goggle Earth objektumai közé „Image Overlay” formátumban”:



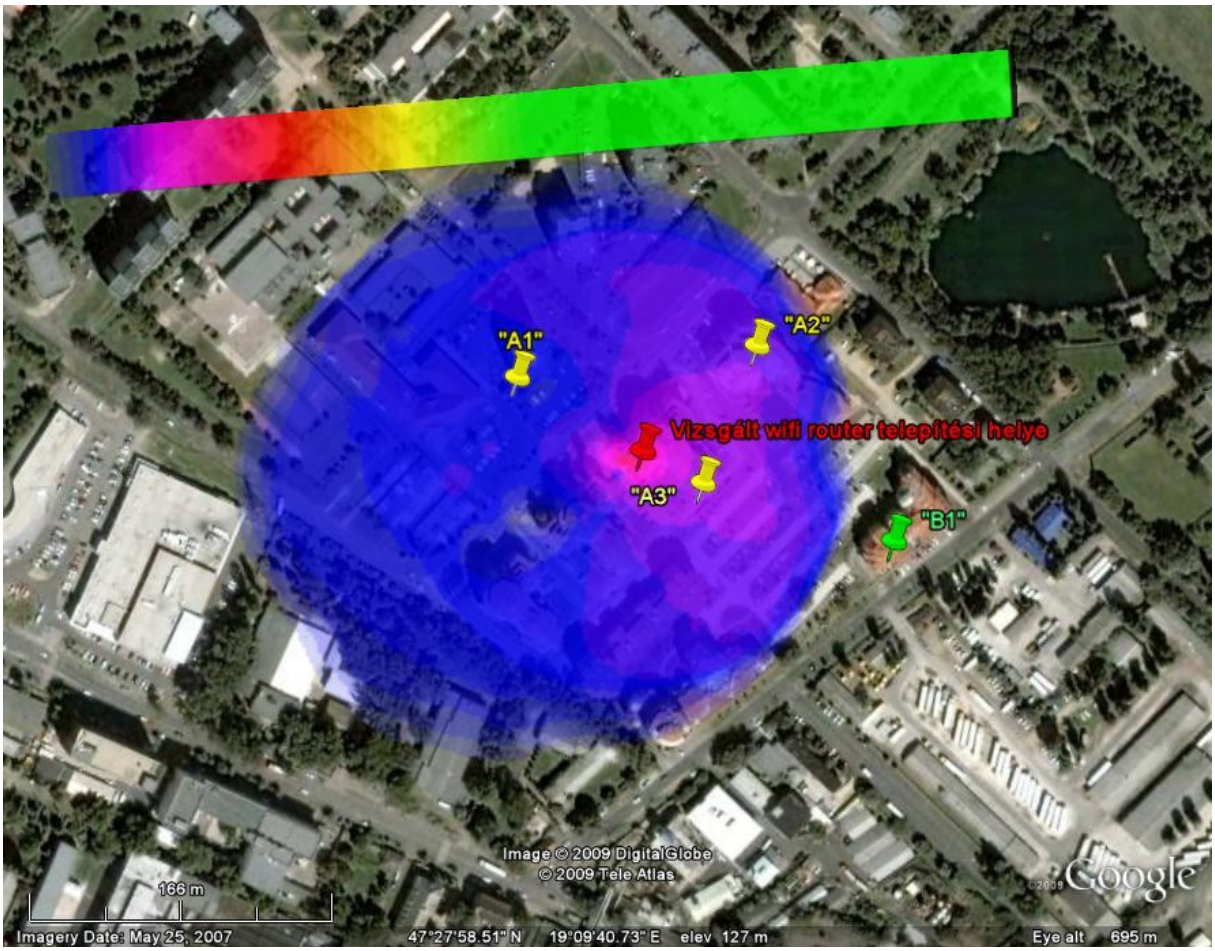
7. ábra. A vizsgált wifi hálózat lefedettsége Footprint segítségével a Google Earthben ábrázolva (forrás: Illési Zsolt)

4) Elemzés

A térképen is megjelenített adatok alapján vizualizálni lehet a vizsgált hálózat karakterisztikáját, megfelelő biztonsággal valószínűsíthetők azok a hálózati elemek (A1, A2, A3), amelyek kapcsolódhatnak a vizsgált hálózati elemhez, illetve kizárhatók azok az eszközök (B1), amelyekről nem vagy csak nagyon kis valósszínűség mellett (pl. speciális antennával felszerelt eszközzel) érhető el a vizsgált végpont.

Az elemzés eredményét színezni is lehet, ami tovább növeli az érthetőséget, és akár egy tárgyalótermi demonstráció során is bemutatható, felhasználva a vád (vagy a védelem) saját verzióinak ismertetéséhez.

Kérdéses esetben a bejárt útvonalon szerzett mérési adatok alapján – a vizsgált végpontéhoz hasonló módon – felrajzolható a többi végpont jelkarakterisztikája is, így kizárhatók az esetleges nem torroid karakterisztika, takarások vagy egyéb tényezők miatt



8. ábra. A vizsgált hálózathoz valószínűsíthetően kapcsolódni képes és nem képes végpontok szétválasztása (és színkódolása)
Google Earthben ábrázolva (forrás: Illési Zsolt)

A vizsgálat során a vizsgált végpont védettsége (védetlen, gyengén védett vagy titkosított volta) és adáskarakterisztikája alapján kimutatható az is, hogy milyen egyéb pontokból valószínűsíthető a hozzáférés, illetve milyen informatikai felkészültséggel és ismeretekkel rendelkező elkövető férhetett hozzá, ami további nyomozati feladatokat generálhat például a lefedett területekkel vagy az elérhető végpontot üzemeltető személyekkel kapcsolatban.

A vizsgálat eredménye alapján megmutatható, hogy ha csak a terhelt férhetett hozzá egy végponthoz, illetve az is, ha rajta kívül többen, több helyről is elérhették és felhasználhatták a végpontot, így mentő bizonyítékot szolgáltathat a terhelt számára.

Az elemzéshez hozzá tartozik azonban az is, hogy az csak a vizsgálat idején megszerzett adatokat tartalmazza, nem ad kapaszkodót arra vonatkozóan, hogy esetleg volt-e korábban olyan technikai körülmény, bekapcsolt hálózati végpont stb. amely lényegesen befolyásolhatja az ügy megítélést.

Összefoglalás

A wifi hálózatok igazságügyi szakértői vizsgálata során elsősorban tárgyi oldali (in rem) – így gyakran közvetlen – bizonyítékok rögzítésére és értékelésére kerül sor, a vizsgálat során a szakértő a támadás forrását jelentő eszközig tudja legfeljebb visszavezetni a bűncselekményeket, fel tudja tárni az elkövetés módját, illetve azonosíthat olyan terhelő és mentő adatokat, amelyek az ügy megítélése szempontjából (pl. szándékosság, gondatlanság) lehetnek relevánsak. Azt azonban ki kell emelnem, hogy az informatikai igazságügyi szakértői vizsgálatok – különösen a wifi hálózatokkal kapcsolatos vizsgálatok – csak több-kevesebb valószínűséggel tudnak az elkövetőre (in personam) vonatkozó bizonyítékokat szolgáltatni.

A cikkemben a vezeték nélküli hálózatok felderítésével és értékelésével kapcsolatos részt elemeztem, áttekintettem a problémákat, illetve egy módszert javasoltam a wifi hálózatok krimináltechnikában is alkalmazható felderítésére, amely akár alapja is lehet egy jövőbeni igazságügyi szakértői módszertani levélnek.

A vezeték nélküli hálózatok felderítése azonban csak része a wifi hálózatokkal kapcsolatos krimináltechnikai vizsgálatoknak.

A felderítés után – akár azzal párhuzamosan is – el kell végezni a hálózati adatforgalom elemzését is, mind a forrás, mind a cél számítógép környezetében. Ez a vizsgálat is halaszthatatlan jellegű, mivel az így megszerezhető bizonyíték (pl. támadást igazoló, vagy törvénysértő tartalmú adatfolyam) egyszeri, a kommunikáció során

A nyomozás során azonban az adatforgalom és az adatnyomokat tartalmazó eszközök a vizsgálatára is ki kell térni, hiszen rengeteg egyéb információt lehet ilyen módon kinyerni, mind a bűncselekménnyel, mind pedig az elkövetés módjával és az elkövetésre felhasznált eszközökkel kapcsolatban.

A „nagy egész”, az informatikai vagy az informatikai eszközökkel kapcsolatos bűncselekmények teljes spektrumának vizsgálata még további elemzések tárgya, amint az is, hogy a technológiai eszközökről és -ből kinyert adatok milyen egyéb nyomozati cselekményekkel köthetők össze az elkövető személyével.

Irodalomjegyzék

[1] 1998. évi XIX. törvény a büntetőeljárásról

[2] 1978. évi IV. törvény a Büntető Törvénykönyvről

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

[4] Detrekői Ákos – Szabó György: Bevezetés a térinformatikába, Nemzeti tankönyvkiadó, Budapest, 1995.

[5] http://www.alyrica.net/sites/default/files/footprint.zip

[6] http://www.netstumbler.org/

[7] Illési Zsolt: Open Source IT Forensics avagy Nyílt forráskódú programok felhasználása az informatikai igazságügyi szakértésben in Bolyai szemle XVII. évfolyam 4. szám (2008-04-01), ZMNE, 2008.

[8] Javvin Technologies, Inc.: Network Protocols Handbook (Third edition), Javvin Technologies, Inc., Saratoga CA 95070 USA, 2006.

[9] Takács Péter - – Rajnai Zoltán: A wifi hálózatok veszélyei in Hadmérnök II. Évfolyam 2. szám, ZMNE, Budapest, 2007.

[10] Tremmel Flórián – Fenyvesi Csaba: Kriminalisztika tankönyv és atlasz, Dialóg Campus Kiadó, Budapest-Pécs, 2002.

[11] wikipedia.org