

## SZÁMÍTÓGÉPES NYOMATOK „TRACKING DOTS” ALAPÚ AZONOSÍTÁSA A BÜNTETŐELJÁRÁSBAN

### 1. A téma indokoltsága

A tanulmány címe ugyan egy jól meghatározott módszer bemutatására utal, az írás tárgyköre ennél bővebb: arra kívánja felhívni a figyelmet, hogy az igazságügyi informatikai szakértői módszerek mit sem érnek, ha a nyomozó hatóság munkatársai nem ismerik ezeket a lehetőségeket, s ez által a büntetőeljárás során releváns adatok kerülhetnek el a bűnjellé, majd bizonyítékká válást.

Tágabb perspektívából tekintve a kérdést, a digitális írástudás és a rendészet kapcsolatát kell vizsgálunk abban a korszakban, amikor a bűnügyi helyszínek a valós és a virtuális térben egyaránt feltűnhetnek, amikor az eszköz használatból eredő digitális nyomok felismerése, vagy szem elől tévesztése döntheti el a büntetőeljárás sikerességét. A következőkben egy olyan eljárás kerül bemutatásra, mely műszaki tartalmát tekintve több évtizedes múltra tekinthet vissza, ugyanakkor napjaink magyarországi büntetőeljárás gyakorlatában új elemként jelenik meg. A témát esettanulmány formájában tekintjük át, mely kapcsán nem csupán a szakértő, de a nyomozó nézőpontját is megismerhetjük.

### 2. A kutatás jogszabályi és műszaki háttere

Az esettanulmányok a valóságban megtörtént események tanulságait gyűjtik össze, s ebből adódóan számos valódi adatot kell tartalmazniuk. Az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény kötelezi a szakértőt a titoktartásra a tudomására jutott tényekre és adatokra vonatkozóan, ugyanakkor fel is hatalmazza azok tudományos vagy oktatási célra történő felhasználására is. Ezt a felhasználást – a jogszabály szerint és a szakértői etikai normák alapján is – meg kell előzni a személyazonosításra alkalmas adatok eltávolításának, mint ahogy az a jelen tanulmányban felhasznált ügyek esetében is megtörtént.

A vizsgálat műszaki környezeteként a címben is meghatározott számítógépes nyomattal összefüggésbe hozható berendezéseket, eszközöket, adathordozókat tekinthetjük. Ezek közül a legfontosabbakat vizsgáljuk meg a következőkben. A számítógépes nyomat létrehozása alapvetően három komponens együtműködését igényli: szoftver (pl. szövegszerkesztő program), hardver (pl. nyomtató) és adathordozó (pl. papír). Az ismertetendő vizsgálati eljárás e három tényezőtől kettőre, a hardverre és az adathordozóra koncentrál. Az adathordozó részletes vizsgálatával keresi a választ arra kérdésre, hogy a nyomatot mely eszközzel készítették, az eszköz milyen gyártmány, illetve mi az egyedi azonosítója a készüléknek. Mindezeket az információkat az adathordozón hátrahagyott nyomtatott elemzésével tárja fel a vizsgálatot végző igazságügyi informatikai szakértő.

Napjainkban ezek a hátrahagyott nyomok négy nyomtatási mód egyikével jönnek létre a leggyakrabban. Ezek közül a legrégebbi és napjainkban egyre kevésbé használt a

impact (ütéses elvű) nyomtatási eljárás, melynek leggyakoribb eszközei dot matrix, a daisy-wheel (margaréta fejű) és line (sor) nyomtatók. Az irodai, vagy a magán használat során az ink-jet (tintasugaras), illetve az electro-photographic elvű eszközök (lézer- és LED nyomtatók) jelennek meg, míg az üzleti (elsősorban a kereskedelmi) területen a thermal elvű eszközök (hőnyomtató) is megfigyelhetők.

A vizsgálati eljárás a tintasugaras és lézernyomtatók által készített nyomatok azonosítására alkalmas, így a továbbiakban e két területtel foglalkozunk részletesen. Mielőtt ezt megtennénk, tisztázni kell, hogy a vizsgálat egyáltalán az igazságügyi informatikai szakértő kompetenciakörébe tartozik-e?

### 3. A szakértői kompetenciakör a számítógépes nyomat azonosításban

Az igazságügyi szakértői szakterületekről a 9/2006. (II. 27.) IM rendelet (Szak. rend.) intézkedik, ahol az informatika vonatkozásában az alábbi szakterületeket adja meg:

1. Informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)
2. Informatikai biztonság
3. Informatikai rendszerek tervezése, szervezése
4. Stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység
5. Számítástechnikai adatbázis, adatstruktúrák
6. Szoftverek

A számítógépes nyomatok vizsgálata az informatikai szakterületen belül a perifériák (1) tárgykörébe tartozik. Ugyanakkor nem hagyható figyelmen kívül az a tény sem, hogy a nyomtatókkal közvetlenül létrehozott – a létrehozás fizikai körülményei által meghatározott – nyomatok vizsgálat a kriminalisztikai okmányszakértő kompetenciakörét is érintheti. Az idézett jogszabály ugyan nem határozza meg tételesen az okmányszakértés konkrét szakterületét, csak annak elnevezését [Szak. rend. 46 § (1) c.]. A tartalmi leírást ezért másodlagos forrásból, a Bűnügyi Szakértői és Kutató Intézet Írás- és Okmányszakértői Laboratóriumának szakterület leírásából idézzük: „A kriminalisztikai okmányvizsgálat kompetenciája a köznyelvi értelemben vett okmányoknál nagyobb körre terjed ki. A leggyakrabban előforduló személyi- és közlekedési okmányokon kívül vizsgálat tárgya lehet például: sorsjegy, bélyeg, postai csekk, boríték, elismervény, szerződés, vagy akár egy - a bűncselekmény helyszínén talált - papírdarab is.

*A leggyakrabban felmerülő kérdések:*

*Az okmány eredeti vagy hamisítvány?*

*Milyen eljárással (nyomdai úton, irodatechnikai eszközök segítségével, egyéb módon) készí-tették?*

*Egyes részeit (pl. adatok, arckép) megváltoztatták, illetve kicserélték-e?*

*Van-e az okmányon látens (szabad szemmel nem látható) írás, tartalma rekonstruálható-e?*

*Valamely bélyegzőnyomat egy meghatározott bélyegzőtől származik-e?*

*Az irat elkészí-téséhez egy, vagy több különböző tollat használtak?”<sup>414</sup>*

A meghatározásból látható, hogy az okmányszakértő joggal tart igényt a vizsgálati szakterületen történő szakértői vélemény kiadás jogára, ugyanakkor nem hagyható figyelmen kívül, hogy az informatikai szakértő – aki a technológiai háttér avatott ismerője –

<sup>414</sup> Bűnügyi Szakértői és Kutató Intézet Írás- és Okmányszakértői Laboratórium honlapja. Forrás: <http://bszki.hu/page.php?295> (Letöltés ideje: 2014.07.18.)

a nyomatok technológiai kialakításával összefüggésben mindenképpen rendelkezik kompetenciával.

A szakértői véleménynek a büntetőeljárásból kompetenciátüllépés miatti kizárása megakadályozható együttes szakértői vélemény kibocsátásával, melynek elkészítése során az okmányszakértő és az informatikai szakértő együttműködik. Ezt a módszert célszerű alkalmazni mindazon ügyek esetén, ahol kétség merül fel a szakértői kompetencia vonatkozásában, akár a kirendelt szakértő, akár a kirendelő hatóság részéről.

#### 4. Számítógépes nyomat azonosítás módszerei

A számítógépes nyomatok azonosítására két alapvető módszer áll a szakértő rendelkezésére: a dokumentumok egyedi jellemzőinek vizsgálatán alapuló ún. passzív technikák, valamint a rejtett információk feltárását célzó ún. aktív technikák.

##### 4.1. Passzív azonosítási technikák

A passzív azonosítási eljárások során a szakértők abból indulnak ki, hogy a nyomtatók előállításánál létrejövő egyedi jegyek (unique characteristics) miatt nincs két egyforma nyomtató, s ez által két egyforma nyomat sem. A különbségeket okozhatják mechanikai eltérések, illetve a működés jellegzetességeiből is adódhatnak. Ez utóbbira közismert példa a lézernyomtatók esetében megfigyelhető csíkozás (banding), melyet a fényérzékeny hengeren megjelenő nagyobb, illetve kisebb töltési szintből adódó eltérő festékmennyiség felvétel okozhat. Az így kialakuló csíkok frekvenciája jellemző lehet az adott nyomtatótípusra, így ha adatbázisba szervezzük a csíkozás mintázatokat, matematikai elemző eljárással azonosíthatjuk a nyomtató típusát.<sup>415</sup>

A passzív technikák közül a szöveges nyomatok karakterkép alapján történő azonosítása emelhető ki. A karakterképzés (különösen a karakter alakját érintő) különbségeit felhasználó vizsgálati módnál a festék túlszóródás (karakter mentén képződő festékmennyiség és minősége), a karakterek szegélyének egyenetlensége, a karakter képzéséhez felhasznált festék mennyisége és még néhány tényező rögzítése és vizsgálata adja kiindulási pontot. A művelet során a karakterkép rögzítése, előfeldolgozása (jellemzők azonosítása és tárolása), majd ezt követően a nyomtatótípusok karakter adatbázisának elemeivel történő összehasonlítást követően a nyomtató típusának azonosítására kerül sor. Az összehasonlító adatbázisnak ebben az esetben is jelentős szerep jut (nagyobb részletesebb adatbázis esetén nagyobb találati arány), amit jelez a vizsgálati mód találati pontossága, mely a paramétereiktől függően 25-82% közötti<sup>416</sup> lehet.

##### 4.2. Aktív azonosítási technikák

Az előzőektől eltérően, amikor a szakértő a nyomatképzés során természetes módon létrejövő jellemzőket vizsgálta, az aktív technikák alkalmazása esetén a nyomtató gyártója szándékolt módon helyez el azonosításra alkalmas jelzéseket a nyomatokon. Ezen módszer nagy mértékben hasonlóságot mutat a biztonsági okmányok jelölésénél alkalmazott

<sup>415</sup> John Mace: Printer Identification Techniques and Their Privacy Implications. University of Newcastle upon Tyne, Computing Science, 2010. 2. o.

<sup>416</sup> John Mace: i. m. 3. o.

megoldásokkal, így nem vitatható, hogy a nyomtatás e típusánál az okmányszakértők ismeretanyagára és tapasztalatára is szükség lehet.

A biztonsági jelölők (security deterrents) esetén amint az angol elnevezésből is következik az elrettentés az elsődleges cél. Az eredetileg minőségbiztosítási célú eljárás jól alkalmazható forenzikus nyomatazonosítások esetén is. A biztonsági jelölő egyfajta színkód, mely keretszerűen helyezkedik el, hat különböző szint alkalmaz a keret 56 részterületén. A szakértők ezekekből a színkódokból képzett ún. funkció vektorok (feature vector) alapján azonosíthatják a nyomtatókat.<sup>417</sup>

A másik kiemelendő aktív technika a nyomkövető kódokkal történő nyomtatás, melynek használata az 1980-as évekre nyúlik vissza, amikor megjelentek az első színes fénymásoló berendezések és lézernyomtatók. A színes nyomtatási technológia vezető cége a Xerox biztonsági jelölést épített be az eszközeibe, tekintettel arra, hogy készülékei papírpénz előállítására is alkalmasak voltak<sup>418</sup>. Ez a biztonsági megoldás a tracking dots (nyomkövető jelek) eljárás, melynek nyomatazonosításban történő felhasználását a következő esettanulmányban mutatjuk be.

#### 4.3. Esettanulmány – tracking dots alapú nyomatazonosítás

A Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatósága nyomozást folytatott az 1978. évi IV. törvény (régi Btk.) 310. § (1) bekezdésben meghatározott és a (4) bekezdése szerint minősülő az adóbevétel különösen nagy mértékben csökkentő adócsalás büntett elkövetésének megalapozott gyanúja. A nyomozás során nagy mennyiségű, számítógépes nyomtatott számla került lefoglalásra, melynek elemzését és az ügy szempontjából lényeges információk (nyomtató azonosító kódja) kinyerését rendelte el a nyomozó hatóság. A szakértőhöz összesen 81 db számítógépes nyomtatott érkezett, mellyel kapcsolatosan a következő kérdésre kellett választ adni: *„I. Nyilatkozzon a szakértő arról, hogy a részére átadott 81 db nyomtatott, eredeti számla számlaképenkénti, tracking dots kódok szerinti vizsgálata alapján a számlákat egy nyomtatóból nyomtatták-e ki. Ennek során, amennyiben lehetséges, a szakértő a nyomtató típusán kívül annak sorozatszámát is állapítsa meg. Továbbá a szakértő tételesen, számlánként állapítsa meg, hogy melyek azok a számlák, amelyek egy nyomtatóból lettek kinyomtatva, és melyek azok, amelyek nem, illetve ez mely számlák esetében nem állapítható meg.”*<sup>419</sup>

A szakértői vélemény idézett része alapján feltételezhető, hogy a nyomozó hatóság munkatársa naprakész a számítógépes nyomatazonosítási technikák területén. E kérdés tisztázása azért is szükséges, mert a büntetőeljárásba bevont szakértők munkájával összefüggő alapvető követelményre világít rá.

Az ügy előadója a kirendelést megelőzően telefonon egyeztetett a szakértővel tekintetben, hogy a számítógéppel előállított számlák azonosítására milyen szakértői módszerek állnak rendelkezésre. Itt szükséges megjegyezni, hogy a nyomozók és a szakértők kapcsolatában meg kell lennie annak a közvetlenségnek, mely alapján a nyomozó

<sup>417</sup> Matthew D. Gaubatz – Steven J. Simske: Printer-scanner identification via analysis of structured security deterrents. in Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on. IEEE, 2009.

<sup>418</sup> John Mace: i. m. 5. o.

<sup>419</sup> Máté István Zsolt: Igazságügyi informatikai szakértői vélemény. szakértői ügyszám: 07/2014. 4. o. (nem nyilvános irat)

mer kérdezni (informatika vagy szakértői eljárást érintő területen), illetve a szakértő válaszol ezekre a kérdésekre.

A szakértő kirendelését megelőzte egy előzetes, személyes konzultáció is, melynek során a szakértő (az ügy részleteinek megismerése nélkül) digitális mintákat vett az vizsgálálandó anyagból, annak megállapítása végett, hogy a nyomatok tartalmaznak-e tracking dot jeleket. A mintavétel eredménye alapján került sor a kirendelésre. Megjegyzendő, hogy az előzetes mintavétel alkalmas lehet a nyomozás során felmerülő költségek mérséklésére, mivel csak abban az esetben érdemes egy vizsgálati eljárást lefolytatni, ha az várhatóan eredményt ad (ez lehet akár kizáró eredmény is). A hasonló esetekben történő előzetes mintavétel (mint a szakértői eljárás megindításának feltétele) fontos része lehetne a büntetőeljárárs nyomozási szakaszának, akár eljárási cselekményként definiálva is.

Az előzetes mintavétel alapján (nyomkövető jelek voltak megtalálhatóak a számlarészleteken digitális mikroszkópkamerás megfigyeléssel) elindult az igazságügyi informatikai szakértői vizsgálat, melynek ismertetését megelőzően szükséges a tracking dots azonosítás részletesebb áttekintése.

A nyomkövető jelek a számítógépes nyomat teljes felületén megjelenő mikroszkópius méretű sárga színű pontok, melyek mintázatszerűen ismétlődnek. A pontok szabad szemmel nem láthatók, csak mintegy hatvanszoros nagyítástól válnak észrevehetővé. A sárga pontok mintázata egy  $8 \times 15$  pontból álló mátrixban rendeződik el, s mivel az azonosítás gyártónként eltérhet, az egyes információblokkok tartalma is különböző lehet. A kódok azonosítását az Electronic Frontier Foundation alapítvány Machine Identification Code Technology (Eszközazonosító kódtechnológia) projektje végezte el, melyet DocuColor Tracking Dot Decoding Guide című tanulmányában hozzáférhetővé is tett.<sup>420</sup>

## 5. A nyomkövető jelek értelmezése

A nyolc sorból és tizenöt oszlopból álló kódtáblázat első sora és első oszlopa az ún. paritás biteket tartalmazza. Ezek olyan hibajelző kódok, melyek segítségével észlelhetők a mátrixban lévő esetleges hibák. Valamennyi oszlop és valamennyi sor (az első sort kivéve) páratlan paritású, ami azt jelenti, hogy az adatbitekből az adott sorban vagy oszlopban páratlan darabszámú helyezkedik el. Abban az esetben, ha az adatbitek páros darabszámúak, a paritás bit 1 értéket vesz fel, egyébként 0 értéket. Az egyes oszlopokban a következő információk kódoltak (balról jobbra):

- 1: paritás bit
- 2: perc érték, a nyomtatás időpontja
- 3-4: használaton kívül
- 5: óra, a nyomtatás időpontja
- 6: nap, a nyomtatás időpontja
- 7: hónap, a nyomtatás időpontja
- 8: év, a nyomtatás időpontja
- 9: használaton kívül
- 10: elválasztó, értéke tipikusan 1 valamennyi pozícióban
- 11-12-13-14: nyomtató sorozatszám binárisan kódolt decimális számmal,

---

<sup>420</sup> DocuColor Tracking Dot Decoding Guide. Electronic Frontier Foundation. Forrás: <https://w2.eff.org/Privacy/printers/docucolor/> (letöltés ideje: 2014.06.06)

## 15: ismeretlen, leggyakrabban üres

A projekt keretében összesen 200 nyomtató vizsgálatára került sor, melyek közül 136 nyomtató esetén sikerült az egyedi azonosítási kódok meghatározása. Az így létrejött adatbázishoz a projekt egy számítógépes programot is kifejlesztett (elérhető a <https://w2.eff.org/Privacy/printers/docucolor/#program> hivatkozáson), mely a kódmintázat megadását követően azonosítja a nyomtatott létrehozó eszközt (amennyiben annak típusa szerepel az adatbázisban).

Az esettanulmányban szereplő ügyre visszatérve, elsőként a számlaképeket tartalmazó nyomtatott egyedi azonosítása történt meg a kirendelő határozatban szereplő felsorolás sorrendjében adott sorszám révén. Ezt követően az egyes nyomatokról egy teljes terjedelmű (A/4 méretű), de alacsony felbontású (600 dpi, mintegy 360 000 képpont négyzethüvelykenként) digitális kép készült 24 bites színmélységgel (> 16 millió szín megkülönböztetésével). A tracking dot azonosítás céljaira a számlakép 3 × 6 centiméteres részlete került digitalizálásra 2400 dpi (mintegy 5,7 millió képpont négyzethüvelykenként) felbontásban, azonos színmélység mellett.

A létrejött digitális állományokat ezt követően a szakértő grafikus szoftverrel dolgozta fel oly módon, hogy a nagy részletességű képen elkülönítette a papír színétől eltérő részleteket egy ún. színmaszk segítségével. A színmaszk érzékenységének módosításával az ún. képzaj kiszűrhető volt az esetek nagy részében. A színmaszkos feldolgozást követően 50 nyomtatott esetben történt további vizsgálat. Ezek a nyomtatott tartalmaztak értékelhető minőségű nyomkövető kódot, a többi nyomtatottól vagy hiányzott a kód, vagy a képzaj miatt nem volt azonosítható.

Az egyes nyomtatottokról kinyert kódokat a szakértő táblázatban ábrázolta, mely alapján elvégezte a típusazonosítást. Megállapítható volt, hogy a mintázat nem szerepel az MICT Projekt adatbankjában, ezért a konkrét nyomtató típus és egyedi nyomtató azonosító megállapítására nem volt lehetőség. A vizsgálat folytatásában a szakértő megvizsgálta, hogy a nyomtatott azonos, vagy különböző eszközökből származnak-e. Ehhez az első vizsgált kódmintázaton felvett egy 19 nyomkövető jelből álló zárt sokszög alakzatot, mely komplexitásából adódóan azonosításra alkalmasnak mutatkozott. A folytatásban a szakértő megvizsgálta, hogy a sokszög alakzat mely nyomtatottokon illeszthető pontosan (darabszám és elhelyezkedés tekintetében egyaránt) a kérdéses nyomtatottokon szereplő tracking dot jelekre. Megállapítást nyert, hogy az alakzat valamennyi, azaz mind az ötven részletes vizsgálat alá vont számlakép részleten pontosan illeszkedik, így a szakértő megállapíthatta, hogy a nyomtatott nagy valószínűséggel azonos eszköztől származtak, de annak típusára vonatkozóan nem tudott nyilatkozni.

A számítógépes nyomtatott azonosítása mellett az egyes ügyekben fontos lehet egy eszköz használatának kizárása is. A Somogy Megyei Rendőr-főkapitányság illetékes bünyügyi szervezeti eleme által történt kirendelés esetében a szakértőnek egy adott eszköz használatára vonatkozóan kellett nyilatkoznia szintén a tracking dots vizsgálati módszer alkalmazásával. A kirendelő határozat szerint a Somogy Megyei Rendőr-főkapitányság Bünyügyi illetékes hatósága nyomozást folytatott a Büntető Törvénykönyvről szóló 2012. évi C. törvény 373. § (3) bek. b) pontjába ütköző és a (2) bekezdés b) pontjának be) alpontja szerint minősülő kisebb kárt okozó üzletszerűen elkövetett csalás büntetettének megalapozott gyanúja miatt. A szakértőnek a következő kérdésre kellett választ adnia: „A szakértő nyilatkozzon arra vonatkozóan, hogy a lefoglalt Konica Minolta magicolor 2400 típusú nyomtatottból kinyomatott tesztoldal és a szintén lefoglalt, és a szakértőnek átadott bűnjelek

(*×××/×××- ×/2014. bü. számú bűnjelek közül: 3,4,6,7,8 -as tételek, ××× feliratú lap 2 db, 2 db ××× feliratú matrica, és 1 db excel táblázatos papírlap*) összevetése alapján azonos e az eredet, illetve így a jelzett nyomtatóból kerültek-e kinyomtatásra.” Ebben az esetben a szakértő kizáró véleménye azon alapult, hogy a kérdéses nyomatokon nem voltak megtalálhatók a nyomkövető jelek, míg a teszt oldalakon a nyomkövető jelek azonosíthatók voltak.

## 6. Összefoglalás

Az ismertetett két eset nem csupán arra világít rá, hogy a nyomozó hatóság és adott esetben az ügyészség és bíróság munkatársai részére is szükségszerű az egyes szakértői módszerek ismerete (a felhasználhatóság felismerésének szintjén), de arra is, hogy a büntetőeljárás nyomozási szakaszában a szakértő és a nyomozó hatóság közötti kommunikáció nem csak az eljárás minőségét, eredményességét, de gazdaságosságát is meghatározhatja. A költséghatékony bűnüldözés a 21. század egyik kihívása lehet, különösen a komplexebbé váló ügyekből adódó növekvő szakértői részvétel miatt. E kihívásokra a helyes válaszokat a gyakorlat és az ezt megalapozó kutatás adhatja meg.