DOI: 10.38146/BSZ.2023.9.5

Anti-forensics technikák szerepe a magas automatizáltságú járművek szakértői vizsgálatában

The role of anti-forensics techniques in the expert examination of highly automated vehicles

Répás József
Dr. doktorandusz
Nemzeti Közszolgálati Egyetem,
Katonai Műszaki Doktori Iskola
repas.jozsef@uni-nke.hu

Absztrakt

Cél: Jelen tanulmány célja a modern járművekhez kapcsolódó szakértői vizsgálatok technikai kihívásainak, illetve az anti-forensics technikák szerepének bemutatása. A magas automatizáltságú járművek katonai alkalmazásban és polgári közlekedésben való széles körű elterjedésével növekszik az utólagos szakértői vizsgálatok szerepe, amelyek célja a jármű igénybevételével, közreműködésével bekövetkezett esemény rekonstruálása, továbbá az esemény elkövetőinek, az eseményben közreműködők vagy érintettek szerepének megállapítása.

Módszertan: A publikáció a vonatkozó angol és magyar nyelvű szakirodalomra, gyakorlati tapasztalatokra, széles körű módszertani forrásanyagokra támaszkodik.

Megállapítások: A magas automatizáltságú járművekben található bizonyítékok, digitális adatok a szakértői vizsgálat céljához kapcsolódóan segítenek megállapítani, hogy milyen esemény, hol, mikor és hogyan történt. Ezekhez az információkhoz való időben történő hozzáférés elengedhetetlen az esemény pontos idővonalának meghatározásához, valamint a kapcsolódó felelősség későbbi megállapításához. Az anti-forensics technikák alkalmazásával lehetőség nyílik a szakértői vizsgálatok kompromittálására, az eredmények minőségének befolyásolására.

Érték: A szakértői vizsgálat lehetőségei és a módszereihez kapcsolódó kiemelt figyelem a tudományos szférában és a médiában egyaránt megjelenik. Egyre több olyan technika jelenik meg, amely késlelteti, nehezíti vagy akár képes megakadályozni az egyes vizsgálati lépések teljes körű végrehajtását. Mint minden módszernek, a szakértői vizsgálatoknak is megvannak a maga korlátai, nehezítő

tényezői, ilyenek például az anti-forensics technikák, amelyek módszerei, hatásai jelen tanulmányban meghatározásra kerülnek.

Kulcsszavak: forenzikus vizsgálat, önvezető járművek, szakértői vizsgálat, anti-forensics

Abstract

Aim: This study aims to present the role of anti-forensics techniques, one of the technical challenges of examinations of modern vehicles. With the widespread use of highly automated vehicles in military and civil transport, the role of forensics examinations is increasing. The purpose of these is to reconstruct the event that occurred with the use and involvement of the vehicle and to establish the role of the perpetrators of the incident, those involved in the event, or those involved in the incident.

Methodology: The publication relies on relevant literature in English and Hungarian, practical experiences, and methodologies from various sources.

Findings: The evidence contained in highly automated vehicles and digital data, related to the purpose of the study, helps to establish what kind of event, where, when, and how it happened. Timely access to them is essential to determine the event's exact timeline and select the related responsibilities. By using anti-forensics techniques, it is possible to compromise expert investigations and influence the quality of the results.

Value: The possibilities of forensics examinations and the special attention related to the methods are also reflected in the scientific sphere and the media. More and more techniques are appearing that delay, complicate, or can prevent the forensics steps. Like all methods, this type of investigation also has limitations and complicating factors, such as anti-forensics techniques, whose methods and effects are defined in this study.

Keywords: forensics examination, autonomous car, expert examination, anti-forensics

Bevezetés

A modern és egyre inkább önvezetővé váló, magas automatizáltságú járművek széles körű elterjedésével a közúti közlekedési rendszerek is fejlődnek, átalakulnak.

A polgári, műveleti és katonai tevékenységek hatékonyságát is nagymértékben befolyásolja, hogy az alkalmazott eszközök, járművek milyen mértékben képesek reagálni a környezet folyamatos változására, segítségükkel milyen módon és mértékben tudjuk előre megtervezni, megszervezni közlekedési feladatainkat, tevékenységünket. Az utóbbi évtized műszaki fejlődésének egyik jelenségeként figyelhető meg, hogy járműveink környezetükről, a valós világról egyre pontosabb, részletesebb információkkal rendelkeznek (Csiszár, Földes & Csonka, 2018). A modern és egyre inkább önvezetővé váló járművek és a közlekedési rendszerek működéséhez, működtetéséhez megfelelő mennyiségű és minőségű információra van szükség. Az új technológiák fejlett infokommunikáció útján biztosítják annak lehetőségét, hogy a járművek számára érzékelhető legyen a környezet, a pálya és azok elemei, a jármű mozgása pedig ezen érzékelt elemek, tárgyak és egyéb külső tényezők mentén valósuljon meg, a jármű ezekhez igazodjon. Különböző kommunikációs csatornák segítségével, a járművek és környezetük összekapcsolásával lehetőség nyílik a környezeti információk és azok hatásainak feldolgozására, ennek megfelelően pedig megvalósítható a járművek irányított térbeli mozgása. Ez a kapcsolat teszi lehetővé, hogy a járművek intelligens közlekedési/információs rendszerben működve képesek legyenek autonóm közlekedésre, a kijelölt hely, úticél elérésére, vagy konvojban való haladásra. „*Az intelligens közlekedési rendszerek olyan fejlett alkalmazások, melyek tényleges (emberi) intelligencia megtestesítése nélkül biztosítanak innovatív szolgáltatásokat a különböző közúti közlekedési módokhoz és forgalmi menedzsmenthez kapcsolódóan*” (URL1). Mind a közlekedési rendszerekben, mind a járművekben olyan alapvető fontosságú információ keletkezik és található, amely a vizsgálat céljának eléréséhez feltétlenül szükséges.

A járművek, illetve a kooperatív intelligens közlekedési rendszerek mint információforrások tekintetében felmerül annak a lehetősége, hogy ezen adatokhoz történő hozzáférés szándékosan korlátozásra kerüljön. Az informatikai rendszerekben egyre több olyan, az elektronikai hadviselésben már alkalmazott technika jelenik meg (például a megtévesztő célok – decoys; hamis bizonyítékok – fake evidences; megtisztítás – cleaning), amely mint ellentevékenység késlelteti, nehezíti vagy képes megakadályozni az egyes vizsgálati lépések teljes körű végrehajtását (Szabó, 2011). A modern járművekhez kapcsolódóan az elkövetett bűncselekmények nyomainak elrejtése, a szakértői vizsgálatok akadályozása érdekében a fenti megoldások közül néhány már jelenleg is rendelkezésre áll, illetve várhatóan a jövőben kifejlesztésre kerül.

Digitális forenzik – digital forensics

A digitális forenzik a kiberbűnözéssel kapcsolatos, digitális eszközökön, vagy bármely számítási képességgel rendelkező eszközön található nyomok visszaállításával és kivizsgálásával foglalkozik. A kifejezést először a számítógépes forenzikkel párhuzamosan, annak szinonimájaként használták, idővel tartalma kibővült olyan eszközökre, amelyek digitális formában tárolnak adatokat. A civil vagy katonai járművekben keletkező, tárolt, továbbított digitális adatok azonosításával, összegyűjtésével, kinyerésével és értelmezésével lehetőség nyílik a járművekhez kapcsolódó múltbeli események vizsgálatára (Gogolin, 2021).

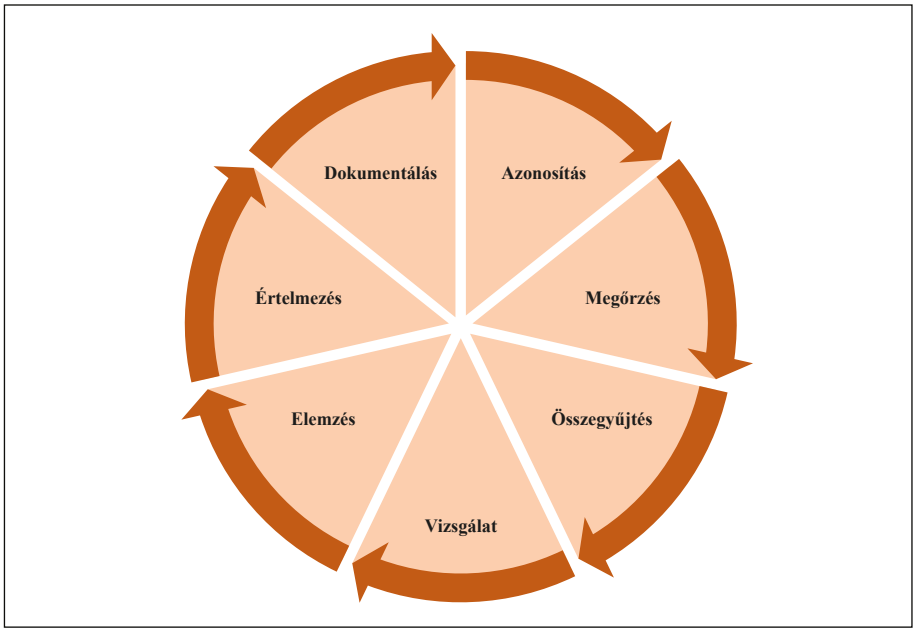
Szakértői vizsgálat lefolytatását több eset is indokolttá teheti, így például egy elszenvedett vagy okozott baleset során a felelősség megállapítása, vagy vitatott tények eldöntése érdekében, egyéb hatósági, jogi, büntetőjogi eljárásban, a nemzetbiztonsági szolgálatok feladatainak ellátásához (például információszerzés, elemzés, értékelés vagy felderítés), továbbá személyek vagy szállítmányok nyomon követése esetén válhat szükségessé. A jármű megjelenhet mint egy cselekmény elkövetésének eszköze, vagy mint egy fizikai vagy logikai támadás célpontja, továbbá tartalmazhat digitális nyomot, bizonyítékot (Chandel, 2020; Kávrestad, 2020; Máté, 2018).

A szakértői vizsgálat során azonosított, megismert információk felhasználhatók például nemzetbiztonságot veszélyeztető cselekmények megelőzésére,[1] jogi eljárásban, katonai műveletekben egyaránt (URL2).

A forenzikus vizsgálat célja a vizsgált eseményhez kapcsolódó, kulcsfontosságú nyomok azonosítása, rögzítése, megőrzése, elemzése, szükséges mértékű utólagos vizsgálata, az eredmények pontos dokumentálása, a bizonyíték hitelességének és sértetlenségének megőrzése, az eredmények laikusok számára is érthető módon történő ismertetése, melyek a digitális forenzikus vizsgálat lépéseit adják.

1 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.

1. számú ábra
Digitális forenzikus nyomvizsgálati lépések



Forrás: A szerző saját szerkesztése.

Anti-forensics

A magas automatizáltságú közlekedési járművek és a kooperatív intelligens közlekedési rendszerek (C-ITS) – részletes, egyes eljárások esetében rendkívül hasznos, más módon pótolhatatlan, nagy mennyiségű információt tartalmazó – adatforrást jelentenek a szakértői vizsgálatok elvégzéséhez. A digitális forenzik egy egyedülálló terület, mert a gyorsan változó információtechnológiai környezetben a szakértők rendre új technikai kihívásokkal néznek szembe. A kihívások megjelenhetnek (hadi)technikai, szoftveres, működési, jogi és nyomozati területen. A digitális forenzikus vizsgálat különböző módszerek, eszközök és technikák alkalmazásával az információk összegyűjtésére koncentrálódik, amelyek alapján rekonstruálható a vizsgálat tárgyát képező esemény, meghatározható annak idővonala, abból felhasználói (és akár egyéb érintettre vonatkozó) adatok ismerhetők meg. Az anti-forensics (mint technikai kihívás) célja, hogy a digitális forenzik keretein belül lefolytatott vizsgálat elvégzését megnehezítse vagy megakadályozza.

Mivel a számítógéppel, digitális eszközökkel elkövetett bűncselekmények (például csalás, hamisítás, adatokban, programokban történő károkozás, jogellenes behatolás, szabotázs stb.) és kibertámadások napjainkban egyre elterjedtebbé válnak, ezek vizsgálatára széles körben elérhetők megoldások. Egyszerűen alkalmazható technikák állnak rendelkezésre a törölt fájlok helyreállítására, fájlrendszerek vizsgálatára. Ezen megoldások folyamatos fejlesztése szükséges annak érdekében, hogy az új technológiák és rendszerek vizsgálhatók legyenek (Mezei, 2018; Gyaraki, 2012).

Ezzel párhuzamosan az úgynevezett elkövetői oldalon is folyamatos a fejlesztés. Törekvésük lényege, hogy a vizsgálatok hatékony lefolytatása ellen olyan megoldásokat dolgozzanak ki, amelyek az adatok, fájlok, naplóállományok, események nyomainak elrejtését, törlését vagy hamisítását végzik. Egyes megközelítésben az anti-forensics megoldásoknak olyan célja is van, hogy kikényszerítik a hatékonyabb forenzik eljárások kifejlesztését, azonban jellemzően a kiberbűnözésben, nyomok eltüntetésében, elrejtésében használatosak. Alkalmazható még nemzetbiztonsági szempontból védendő dokumentumok védelmére, nyomok elrejtésére, fedett információgyűjtésre, vagy személyes adatok vagy dokumentumok védelemre is.

Az anti-forensics módszerek alkalmazásában érintett személyek (támadók, védekezők vagy elkövetők), olyan folyamatok és eszközök kombinációját alkalmazzák, amelyek a vizsgálati feladatok végrehajtásának akadályozását célozzák. Az anti-forensics eszközök, eljárások és technikák folyamatosan bővülő gyűjteménye a rendszereken lévő adatok azonosítását, az azokhoz történő hozzáférést, bizonyítékok gyűjtését megnehezítik, meghiúsítják vagy hátráltatják a szakértő vizsgálatok végrehajtását, és rendre kihívások elé állítják a szakértőket. Ide tartozik minden olyan tevékenység, amelyek célja az esemény, tevékenység, támadás nyomainak elrejtése, vagyis különböző módszerek és technikák felhasználásával igyekeznek elrejteni vagy módosítani a nyomokat a vizsgálat hátráltatása érdekében.

Amíg a szakértői vizsgálatok során mindent elkövetnek azért, hogy a digitális eszközökről hiteles bizonyítékokat nyerjenek ki, addig az anti-forensics oldalon megpróbálják elrejteni, illetve megsemmisíteni azokat.

Míg a számítógépes környezetben használható vizsgálati eszközök, technikák, módszerek vagy egyes folyamatlépések részben vagy egészben alkalmazhatóak a mai modern járművekben is, az egyre inkább önvezetővé váló járművek esetén, a komplex működésből és felépítésből adódóan, azonban korlátozott módon lesznek használhatóak. Az anti-forensics technikák használata a katonai célú és polgári közlekedési járművek vonatkozásában napjainkban még nem terjedt el, azonban a szakértőknek időben fel kell készülnie az új kihívásokra, melyeket

az új közlekedési járművek hoznak magukkal ezen a területen is (Répás, Schmidt & Berek, 2022; Gogolin, 2021; URL3; URL4; URL5; URL6).

Anti-forensics taktikák, technikák és eljárások

Az anti-forensics taktikák, technikák és eljárások (TTPs – tactics, techniques and procedures) elrejtik vagy minimalizálják a felhasználók tevékenységének nyomait (digitális lábnyomot), megnehezítik vagy megakadályozzák a kapcsolódó bizonyítékok azonosítását, megszerzését, kihasználják a forenzik eszközök gyengeségeit, hibáit, továbbá bonyolulttá és időigényessé teszik a szakértői vizsgálatok elvégzését, vagy megpróbálják félrevezetni, lehetetlenné tenni azt. Az ilyen megoldások elkövető oldali alkalmazásának célja:

- (meg)akadályozni a szakértői vizsgálat lépéseit,
- a szakértői munka elnyújtása, nehezítése,
- szakértők félrevezetése, megtévesztése,
- nyomok elrejtése, kinyerésének akadályozása,
- jelentés pontosságának és hitelességének megkérdőjelezése,
- a forenzik eszköz (tool) használatának nehezítése,
- a forenzik eszköz (tool) használatának, jelenlétének felfedése,
- a forenzik eszköz kompromittálása, támadó eszközként való felhasználása,
- közvetlen támadás a szakértő ellen,
- az anti-forensics eszköz nyomainak törlése.

Ezekkel csökkentik a releváns digitális bizonyítékok mennyiségét és minőségét is (Gogolin, 2021; URL11; Grupal, 2014; Simon, 2007).

A szakértői vizsgálat lépéseinek akadályozása, meghiúsítása alatt a folyamat fő lépéseinek – a digitális bizonyítékok kinyerésének, az összegyűjtött adatok feldolgozásának, ellenőrzésének vagy elemzésének – negatív befolyásolását értjük (Prabin, 2019). A felsorolásra kerülő példák jellemzően számítógépes környezetből származnak, mivel a járművek esetén ilyen megoldások még nem készültek vagy nem terjedek el.

Az adatok elrejtése egy régi módszer, amelynek célja az adatok észrevehetetlené, észlelhetetlenné tétele, miközben még jelen vannak az adattárolón. Megvalósítható az adatok áthelyezésével olyan helyre, ahol a szakértői vizsgálat során esetleg nem keresik, vagy hordozható eszközre helyezik át. Ezek az áthelyezések azonban nyomot hagynak maguk után, az adatátvitel ténye és a hordozható eszközök használata megjelenik a naplófájlokban. Emellett a szakértői vizsgálat során a fizikai vagy logikai lemezképek teljes tartalma kerül vizsgálatra, az

elemző szoftverek a teljes adathalmazt vizsgálják, így az adathordozón belüli áthelyezés kevéssé hatékony megoldás. A szakértői munka azonban nem elvégezhető például PIN vagy jelkóddal vagy biometrikus adattal védett mobiltelefonon, amennyiben ezek nem ismertek vagy állnak rendelkezésre.

A munka elhúzódhat, speciális vagy nem elterjedt (például ZFS) fájlrendszer, operációs rendszer (például járművekben a Windows Automotive) vagy tiltott fájlnevek (például CON, PRN, AUX, NUL, COM1, COM2 stb.) alkalmazása esetén (URL7). A nem általánosan használt RAID vezérlők alkalmazása, egyedi RAID paraméterek használata miatt rendkívül időigényes lehet az egyes variációk kipróbálása, a vizsgált eszközön nem mindig valósítható meg a RAID tömbök összeállítása.

A nem elérhető hálózati meghajtó félrevezetheti, megtévesztheti a szakértőt, ami hátráltatja és megnehezíti munkáját. Az adattelítéssel vagyis a használt, nagy számú adathordozó (HDD-k, USB kulcsok, CD-k, DVD-k, mobil eszközök) megőrzésével és rendszeres használatával lassítható az adatgyűjtés folyamata, mivel minden egyes eszköz vizsgálata szükségessé válik (URL8). A vizsgálati célból lefoglalt eszköz, vezeték nélküli kapcsolaton keresztül (például wifi, Bluetooth), az eszközhöz történő közvetlen fizikai hozzáférés nélkül, távolról is törölhető, megakadályozva ezzel a vizsgálat elvégzését.

A nyomok elrejtésére kriptográfiai, szteganográfiai módszerek vagy obfuszkáció alkalmazhatóak. A kriptográfia vagy rejtjelezés „*feladata matematikai módszereket alkalmazó algoritmusokkal és azok használatának pontos leírását tartalmazó – szigorúan betartandó – kriptográfiai protokollok segítségével biztosítani az üzenetek, illetve tárolt információk bizalmasságát, védettségét, hitelességét*” (Muha & Krasznay, 2018). A szteganográfia az üzenetek elrejtésének tudománya. Míg a kriptográfiai megoldásokkal a továbbított üzenet meglétét nem titkoljuk, maga az üzenet titkosított formában kerül továbbításra, a szteganográfia segítségével nem a továbbítandó üzenet adattartalma kerül elrejtésre, hanem magának az üzenetnek a létezését titkoljuk (Bertók, 2010; Földes, 2009). Az obfuszkáció anti-forensics értelemben szándékos elrejtést jelent, annak érdekében, hogy a vizsgálatot végző szakértő számára zavaros, kétértelmű vagy nehezen érthető legyen az adattartalom. *„Szoftverek esetében ezt a kiadott binárisra tudjuk értelmezni, azaz minél nehezebben lehessen megérteni annak pontos működését úgy, hogy a program helyesen működik*” (Kócsó, 2004). Segítségével a kártékony kódok elrejthetők, továbbá védhetővé válik az algoritmus, megakadályozható az illegális szoftvermásolás, nehezíti a kód és a tartalom megértését és visszafejtését (Kócsó, 2004).

A vizsgálat során gyűjtött digitális bizonyítékok olyan adatok („*bizonyító erejű információk, amelyeket bináris formában tároltak, vagy továbbítottak*”), amelyek

a vizsgálat szempontjából releváns tényekre vonatkoznak, olyan forrásokból származnak, ezeket olyan bizonyítási eszközökből szerezték be (megismerhetővé váltak), amit jogszabály lehetővé tesz. „*A digitális bizonyíték megismerhető:*

- *megkereséssel (Be. 71. §);*
- *az adathordozónak, illetve az adatnak a lefoglalásával (Be. 151. §);*
- *információs rendszerben tárolt adatok megőrzésére kötelezéssel (Be. 158/A §);*
- *titkos információgyűjtéssel (1994. évi XXXIV. törvény a rendőrségről 63. §); illetve*
- *titkos adatszerzéssel (Be. 200–202. §)*" (Sorbán, 2016).

„A bizonyítási eszköz tehát a bizonyíték hordozója, a bizonyíték pedig az az információ, amelyhez a bizonyítási eszközből jutunk" (Sorbán 2016). Az anti-forensics technikák segítségével befolyásolható a digitális bizonyítékokhoz való hozzáférés, azok relevanciája vagy hitelessége, ezáltal a teljes vizsgálati jelentés megfelelőssége is. A jelentés vagy annak adattartalmának pontossága és hitelessége nagyban függ továbbá attól, hogy az adatokról készült másolat hiteles-e, pontosan (például a rendszeridő pontossága, hiteles külső időforráshoz való szinkronizációja) és teljeskörűen tartalmazza-e a bizonyíték tartalmát, valamint, hogy a másolaton minden releváns adat megtalálható-e, ami az eredeti adathordozón megtalálható volt (Fülöp, 2020). A vizsgálatok során a fájlrendszer időbélyegei alapján, az úgynevezett MACE idők (Modified, Accessed, Created, Entry), a fájlok utolsó módosításának, olvasásának, készítésének és az MFT (master file table) rekord utolsó frissítési dátumának felhasználásával kerül összeállításra az események idővonala. Azonban ezen idők módosíthatók vagy beállíthatók véletlenszerűen is, ami hátrányosan befolyásolja a vizsgálati eredmények megfelelősségét és hitelességét (URL8).

A szakértő forenzikus eszköznek használhatóságát nehezíti vagy eredményességében korlátozzák az anti-forensics megoldások. A vizsgálandó rendszerben, annak működés közben keletkező illékony adatok, az alkalmazások futtatása során a memóriában található információk (például futtatott szolgáltatások, esemény naplók) megszerzése, az adatok feldolgozása és vizsgálata a live forensics feladata (URL9; URL10; Adelstein, 2006). Az ideiglenes memóriában található adatokhoz való hozzáférés például olyan megoldással is akadályozható, hogy az anti-forensics alkalmazás monitorozza az USB portokhoz csatlakoztatott eszközöket, amennyiben egy nem regisztrált eszköz kerül csatlakoztatásra, a teljes memória területet (vagy csak egy részét), továbbá az adathordozó tartalmát tetszőleges (logikai 0-kal és 1-ekkel) vagy véletlenszerű adattartalommal felülírja. Tekintettel arra, hogy az illékony adatok egyrészt működés közben változhatnak,

másrészt az eszköz kikapcsolását (a jármű áramtalanítását) követően a memória sajátosságai miatt elvesznek, ezért a múltbeli esemény rekonstruálása e technológia használatával csak rendkívül korlátozott időtartamban lehetséges. Az időtartam függ a szoftver működésétől – pár másodperces, illetve esetleg néhány órás időtávra korlátozódik. A live forensics megismételhető szituációban, például az esetleges gyártói szoftver üzemzavarára, hibás működésére deríthet fényt. Ennek megfelelően a live forensics kizárólag speciális esetekben, a pontos, szoftveres megismételhetőség miatt rendkívül korlátozottan alkalmazható járművek esetében.

A Zero-Footprinting (nulla lábnyom) eszköz viszonylag új anti-forensics megoldás, ami az adattárolók „megtisztítására" vagy a lemez eredeti tartalmának teljes megsemmisítésére használható, ezáltal a támadást teljesen észrevehetetlenné teszi. A forenzik eszköz használatának, jelenlétének felfedése, például kártékony kódok működési mechanizmusának szakértő általi feltárása során lehet fontos (anti-forensics szempontból). Annak érdekében, hogy a kártékony kód a jelenlétét elrejtse, működését felfüggesztheti például, ha virtuális gépen történő futtatást észlel.

Magának a forenzik eszköznek a visszatámadásra való felhasználása akadályozhatja a nyomok elemzését és utólagos vizsgálatát. Mivel a forenzik eszközök (például hálózati forgalomelemzők) nagyban segítik a vizsgálat elvégzését, a következtetések levonását, ezek sérülékenységeit kihasználva hiba generálható a működésükben. Puffer túlcsordulás támadás indításával vagy tetszőleges kódok futtatásával akadályozható az eszközök működése, vagy az általuk használt erőforrások túlterhelésével a teljes vizsgáló környezet rendelkezésre állása negatívan befolyásolható (Chhabra, 2014).

A vizsgálat akadályozásának egyik módja a szakértő elleni közvetlen logikai vagy fizikai támadás. Logikai támadásként, elektronikai ellentevékenységként értelmezhető a szakértő informatikai hálózata ellen irányuló felderítés vagy a kapcsolat megszakítására irányuló tevékenység; fizikai támadás lehet a szakértő közvetlen megtámadása vagy a vizsgálat helyszíne (például épület) ellen irányuló kinetikus támadás (Garfinkel, 2007).

A szakértői vizsgálat lefolytatásának vagy eredményeinek befolyásolására alkalmazott anti-forensics eszközök nyomainak törlése összetett feladat, például az operációs rendszerek több szintű naplózása miatt. Az egyes műveletek elvégzését, alkalmazások futtatását több helyen és módon rögzíti az operációs rendszer, ezért a nyomok teljes eltüntetése nem minden esetben valósítható meg teljeskörűen. Még az adatok wipe-olása, vagyis a biztonságos, felülírással történő törlése is több helyen (registry-ben, journal fájlban, auditnaplóban stb.) hagy nyomot, ezért a vizsgálat során nélkülözhetetlen a körültekintő feladatvégzés.

Anti-forensics megoldások alkalmazhatósága a digitális forenzik lépéseiben

A szakértői vizsgálat során különböző technikai nehézségek, nehezítő tényezők merülhetnek fel (például a fentebb tárgyalt megoldások), amelyek a vizsgálatokat hátráltatják, vagy rendkívüli erőforrás-felhasználást (például idő, eszköz, pénz) eredményezhetnek, megnövelve ezzel a vizsgálat idejét és költségeit. Az adatok tárolási helye és módja, az inkompatibilitás és az adatmennyiség mellett, a technikai kihívások egyik fő csoportját alkotják a különböző anti-forensics megoldások.

Az alkalmazott anti-forensics technikától, taktikától, eljárástól függően lehetőség nyílik az egyes vizsgálati lépések akadályozására, elnyújtására, meghiúsítására, a szakértő félrevezetésére, a vizsgálat pontosságának, hitelességének megkérdőjelezésére. Az 1. számú táblázatban látható, hogy a modern járművek utólagos szakértői vizsgálatában, a digitális forenzik egyes lépései esetén milyen lehetőségeket nyújtanak az anti-forensics megoldások.

1. számú táblázat
Digitális forenzik lépései és a kapcsolódó anti-forensics célok

Digitális forenzik	Anti-forensics
Azonosítás	Elrejtés, félrevezetés, elnyújtás
Megőrzés	Törlés, akadályozás, elnyújtás
Összegyűjtés	Akadályozás, elnyújtás
Vizsgálat	Félrevezetés, meghiúsítás, elnyújtás
Elemzés	Félrevezetés, pontatlanítás, elnyújtás
Értelmezés	Akadályozás, hiteltelenítés, elnyújtás

Forrás: A szerző saját szerkesztése.

A járműben keletkező, gyűjtött, továbbított és tárolt adatok, vagyis a nyomok elérhetősége és használhatósága elsődleges a szakértői vizsgálat elvégzésében. A támadók vagy elkövetők egyre kifinomultabb technikákat alkalmaznak annak érdekében, hogy megnehezítsék az egyes digitális forenzik lépések végrehajtását. A mai modern járművek vonatkozásában, a digitális adatok tárolási helyének azonosítása viszonylag „egyszerű” feladat. A járműgyártók hasonló, standardizált megoldásokat alkalmaznak az egyes adatkörök tárolására. A különböző elektronikus vezérlő egységek (ECU – electronic control unit), jármű fejegység és eseményadat-rögzítő (EDR – event data recorder) szolgálnak a jármű működéséhez és működtetéséhez szükséges adatok tárolására. Ezek a megoldások várhatóan a jövőben, a járművek belső felépítésének központosításával (central

brain alkalmazásával) sem változnak meg nagy mértékben, a súlypont tevődik majd át az egyes elemekről a központi egység irányába. Ennek fényében, a számítógépes szakértői vizsgálatokkal ellentétben, a járművek vizsgálata esetén a nyomok tárolási helyének azonosítása nem lesz befolyásolható anti-forensics megoldásokkal, ellenben a releváns adatok azonosítása igen.

Az adatok megőrzését az egyre modernebb adattároló megoldások fogják biztosítani, az egyes járműtípusokban napjainkban is használt HDD-k és a mozgó alkatrészt tartalmazó adattároló helyett elterjednek az SSD-k és különböző memóriakártya megoldások. A felhő alapú rendszerek megállíthatatlan(-nak tűnő) terjedése a járműiparban is új megoldásokat fog eredményezni. Ezek alkalmazása megnehezítheti a nyomok megőrzését.

Az adatok összegyűjtését a használt technológiák változatossága, az inkompatibilitási problémák mellett az anti-forensics megoldások is nehezíteni fogják. A vizsgálat hitelességének és pontosságának, az elemzés megfelelőssége, a téves következtetések levonása tekintetében a járművek esetén is nagy hangsúlyt kell fektetni az anti-forensics megoldások ellensúlyozására.

Míg a szakértői vizsgálatok az egyes lépések teljeskörű, pontos és hiteles végrehajtását célozzák, addig a támadói, elkövetői oldalon ezek minőségének, hatékonyságának csökkentésére irányuló célok találhatók.

Összefoglalás

A modern és egyre inkább önvezetővé váló közúti közlekedési járművek katonai és polgári felhasználási köre várhatóan nagy mértékben bővülni fog. A jármű-érintettségű események utólagos szakértői vizsgálataiban rekonstruálni kell a történteket, meg kell állapítani az esemény elkövetőinek, az eseményben közreműködők vagy érintettek szerepét. Ehhez a járművekben található digitális adatok segítségével rekonstruálható az esemény idővonala, és hogy mi, mikor, hogyan történt. Az anti-forensics technikák, taktikák és eljárások nem csupán a számítógépes vizsgálatok esetén jelennek meg, a modern járművekhez kapcsolódóan is képesek lesznek nehezíteni a nyomok azonosítását, az adatok kinyerését, összegyűjtését, a vizsgálati lépések végrehajtását.

Felhasznált irodalom

Adelstein, F. (2006). Live forensics: Diagnosing your system without killing it first. *Communications of the ACM, 49*(2), 63–66. http://dx.doi.org/10.1145/1113034.1113070

Bertók Zs. (2010). *Szteganográfia.* Budapesti Műszaki és Gazdaságtudományi Egyetem.
Chandel, R. (2020). *Digital forensics: An Introduction*. Hacking Articles.
Chhabra, G. S. & Jani, A. (2014). *Anti-Forensics Techniques: An Analytical Review.* 2014 Seventh International Conference on Contemporary Computing (IC3). https://doi.org/10.1109/IC3.2014.6897209
Csiszár Cs., Földes D. & Csonka B. (2018). *Közlekedési információs rendszerek*. Akadémia Kiadó. https://doi.org/10.1556/9789634542773
Földes Á. M. (2009). *Szteganográfiai algoritmusok vizsgálata*. Műszaki és Gazdaságtudományi Egyetem.
Garfinkel, S. (2014). *Anti-Forensics: Techniques, Detection and Countermeasures.* The 2nd International Conference on i-Warfare and Security (ICIW). Naval Postgraduate School. https://doi.org/10.1109/IC3.2014.6897209
Gogolin, G. (2021). *Digital Forensics Explained. CRC Press.* https://doi.org/10.1201/9781003049357
Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer. https://doi.org/10.1007/978-3-030-38954-3
Kócsó B. (2014). *Szoftverek obfuszkációja*. Budapesti Műszaki és Gazdaságtudományi Egyetem.
Máté I. Zs. (2018). Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. *Belügyi Szemle, 66*(7-8), 36–54. https://doi.org/10.38146/BSZ.2018.7-8.3
Muha L. & Krasznay Cs. (2018). *Az elektronikus információs rendszerek biztonságának menedzselése*. Nemzeti Közszolgálati Egyetem.
Prabin, K. S. (2019). *Forensics analysis of client-side artifacts on cloud based application*. Tallinn University of Technology.
Répás, J., Schmidt, M. & Berek, L. (2022). *Autonomous Vehicles Forensics – The next step of the Digital Vehicles Forensics*. 1st IEEE International Conference on Cognitive Mobility.
Sorbán K. (2016). A digitális bizonyíték a büntető eljárásban. *Belügyi Szemle, 64*(11), 81–96. https://doi.org/10.38146/BSZ.2016.11.5
Szabó A. (2011). Preventív hálózatvédelmi rendszerek alkalmazási lehetőségei a támadások detektálására, valamint a módszerek elemzésére 1. rész. *Hadmérnök, 4*(4), 239–249.

A cikkben található online hivatkozások

URL1: *Az Európai Parlament 2010/40/EU irányelve*. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32010L0040&from=HU
URL2: *How Well Do You Know Digital Forensics?* https://www.eccouncil.org/what-is-digital-forensics/
URL3: *Vehicle Forensics.* https://www.linkedin.com/pulse/what-exactly-vehicle-forensics-carly-mcgee

URL4: *Countering anti-forensics efforts – part1*. https://belkasoft.com/countering-anti-forensic-efforts-part-1
URL5: *Understand Anti-forensics and their goals.* https://info-savvy.com/understand-anti-forensics-and-their-goals/
URL6: *Sophisticated Anti-Forensic Tactics and How To Spot Them*. https://www.kroll.com/en/insights/publications/cyber/anti-forensic-tactics
URL7: *Naming Files, Paths, and Namespaces*. https://learn.microsoft.com/en-us/windows/win32/fileio/naming-a-file
URL8: *Anti-Forensics and Anti-Anti-Forensics*. https://infocon.org/cons/DEF%20CON/DEF%20CON%2020/DEF%20CON%2020%20presentations/DEF%20CON%2020%20-%20Perklin-AntiForensics.pdf
URL9: *What is Live Forensics.* https://www.igi-global.com/dictionary/a-compendium-of-cloud-forensics/82342
URL10: *Incident Response: Live Forensics and Investigations*. https://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Incident-Response-Live-Forensics-and-Investigations.pdf
URL11: *Countering Anti-Forensic Efforts*. https://www.forensicfocus.com/articles/countering-anti-forensic-efforts-part-1/

Alkalmazott jogforrás

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

A cikk APA szabály szerinti hivatkozása

Répás J. (2023). Anti-forensics technikák szerepe a magas automatizáltságú járművek szakértői vizsgálatában. *Belügyi Szemle*, *71*(9), 1607–1620. https://doi.org/10.38146/BSZ.2023.9.5