

A magas automatizáltságú katonai és polgári közlekedési járművekben megtalálható digitális adatok hozzáférhetőségének és értelmezhetőségének kihívásai

A digitális forenzikus vizsgálatok különféle módszereket, eszközöket és technikákat foglalnak magukban, amelyek kulcsfontosságúak a polgári és a fegyveres erők esetén is a digitális bizonyítékokhoz való hozzáféréshez, azok vizsgálatához és elemzéséhez. A járművek folyamatos fejlődésével, automatizáltsági szintjük növekedésével a működésük, valamint a segítségükkel történő feladatellátás egyre szélesebb körű adatforrásokat, -feldolgozást és -kezelést igényel. A járművek által különböző informatikai rendszerekből és rendszerelemekből gyűjtött, a járműben vagy a kapcsolódó rendszerekben tárolt és jellemzően vezeték nélküli kommunikációs csatornán továbbított adatok hozzáférhetővé tétele, valamint az adatok feldolgozása és értelmezése új kihívást jelent a szakértők számára. Tanulmányunk célja meghatározni a modern közlekedési járművek szakértői vizsgálata során elérhető adatok hozzáférési módjait, kihívásait és lehetőségeit.

Kulcsszavak: forenzikus szakértői vizsgálat, önvezető járművek, szakértői vizsgálat

THE CHALLENGES OF ACCESSIBILITY AND INTERPRETABILITY OF DIGITAL DATA FOUND IN HIGHLY AUTOMATED MILITARY AND CIVILIAN TRANSPORT VEHICLES

Digital forensics encompasses a variety of methods, tools, and techniques that are key to accessing, examining, and analysing digital evidence for both civilian and military forces. With the continuous development of vehicles and the increase in their level of automation, their operation and the performance of tasks with their help require a wider range of data sources, data processing, and management. The accessibility of data collected, and stored by vehicles from the environment, different IT systems, and system components, are typically transmitted via wireless communication channels. The processing and interpretation of data pose a new challenge for experts. The aim of this study is to identify the methods, challenges, and opportunities of accessing the data available during the expert examination of modern transport vehicles.

Keywords: forensics examination, autonomous vehicles, vehicle examination

Bevezetés

A katonai műveletekhez kapcsolódó logisztikai feladatokban és a polgári közlekedésben egyaránt megjelennek a magas automatizáltságú, modern, professzionális technológiai eszközökkel felszerelt járművek. Működésük alapját a rendkívül gyors adatgyűjtő és -feldolgozó képesség, valamint a fejlett kommunikációs megoldások képezik. A modern járművek adatfeldolgozása három fő feladatcsoport köré épül. Egyrészt a környezetérzékelés: a jármű különböző szenzoraiból (kamera, lézer, radar, ultrahang stb.) alkotott érzékelőhálózat folyamatosan felméri a környezet változását. Célja a környezetről olyan pontos és megbízható modell előállítása, amely lehetővé teszi a szituációértékelést. A környezeti modell alapján a jármű értékeli az adott közlekedési szituációt a megfelelő döntéshozatal és a jármű-irányítási feladat elvégzése érdekében.

Az autonóm járműirányítás a katonai műveletekben hozzájárul az emberi erőforrás megóvásához, javítja a műveleti képességeket és azok hatékonyságát (például megfigyelés, környezetdetektálás, támadási feladatok stb. esetén). Ezzel szemben a polgári felhasználásban a közlekedés biztonságosabbá tételén és a felhasználók mindennapi életének komfortosabbá tételén van a hangsúly. Főként a rövid távú, akár rögzített útvonalon közlekedő (például minibusz-szolgáltatás, ipari szállító járművek stb.) járművek felhasználása terjedt el, megjelennek az önvezető taxik, a csak autópályán használható önvezető funkciók. 2024 nyarától pedig tesztelési célból már megjelenhetnek a SAE J3016-os szabvány szerinti 4-es szintű, önvezetőnek számító járművek Peking utcáin. A közlekedésbiztonsági szempontokat is figyelembe véve, valamint a többi jármű vezetőjének figyelmét felhívandó az önvezető funkciókat használó autókát türkizkék megkülönböztető lámpáikról lehet felismerni.¹

„A SAE J3016 számú nemzetközi szabványa hat szintet határoz meg a polgári felhasználású közlekedési járművek vezetésautomatizáltságára. Az első három szinten (SAE 0-2) a jármű vezetője felügyeli az eseményeket, a második három szinten (SAE 3-5) maga a jármű végzi mind a felügyeleti, mind a jármű vezetési feladatait.”²

A digitális forenzikus vizsgálatok különféle módszereket, eszközöket és technikákat foglalnak magukban, attól függően, hogy milyen célból (például adat- és információszerzés, elemzés-értékelés, műveleti tevékenység támogatása, szakértői vizsgálat stb.) milyen eszközök vagy rendszerek vizsgálatát kell elvégezni. Mind

¹ GÁSPÁR-NÉMETH-BOKOR 2019; SIMON 2024; Autopro.hu/R.K.E. 2024.

² BEREK L. – BEREK T. – RÉPÁS 2023.

polgári, mind katonai vonatkozásban a digitális nyomokhoz való hozzáférés kulcsfontosságú feladat, azok vizsgálatához és elemzéséhez.

Modern járművek az adat- és információszerzési területeken

A járművek folyamatos fejlődésével, automatizáltsági szintjük növekedésével működésük, valamint a segítségükkel történő feladatellátás egyre szélesebb körű adatforrásokat, -feldolgozást és -kezelést igényel. A járművek által különböző informatikai rendszerekből és rendszerelemekből gyűjtött, a járműben vagy a kapcsolódó felhőalapú rendszerekben tárolt és jellemzően vezeték nélküli kommunikációs csatornán továbbított adatok hozzáférhetővé tétele, valamint az adatok feldolgozása és értelmezése új kihívást jelent a szakértők számára, amelyre megoldást jelentenek a különböző információszerzési megoldások.

Az adat- és információszerzés sikerét modern járművekhez kapcsolódóan alapvetően a hozzáférhető és megszerezhető adatok mennyisége befolyásolja. A nagyobb adatmennyiség nem feltétlenül növeli az információ értékét, a vizsgálatok lefolytatását a túl sok információ meg is hiúsíthatja. Megnehezíti a releváns információk feltárását, lassítja az adatfeldolgozást, az elemzést és az értékelést.

A modern járművekhez kapcsolódóan az adat- és információszerzés területei a műveleti vagy vizsgálati cél függvényében relevánsak lehetnek, azonban a képességek hatékony felhasználása érdekében és az időprés miatt a gyakorlatban csak azokat a módszereket alkalmazzák, amelyek a leghatékonyabban biztosítják a szükséges adatok és információk megszerzését. Alkalmazható információszerzési területek:

- emberi erőforrásokkal folytatott információ- és hírszerzés (*Human Intelligence, HUMINT*);
- rádióelektronikai felderítés (*Signals Intelligence, SIGINT*);
- nyílt forrású információszerzés (*Open Source Intelligence, OSINT*);
- képfelderítés (*Imagery Intelligence, IMINT*);
- mérés- és jelmeghatározó hírszerzés (*Measurement and Signature Intelligence, MASINT*);
- technikai hírszerzés (*Technical Intelligence, TECHINT*);
- kiberhírszerzés (*Cyber Intelligence, CYBINT*).

Polgári alkalmazásban, ideális esetben a járművekkel kapcsolatos adat- és információszerzési feladatok a felhatalmazáson alapuló, utólagos szakértői vizsgálatokat

jelentik. A felhatalmazást a megbízási vagy vállalkozási szerződés, továbbá a kirendelő határozat vagy bírósági végzés jelenti, amely tartalmazza az adatigényt, a megválaszolandó szakértői kérdéseket.

A felhatalmazás és jogosultság nélküli, a járművek belső adataihoz való hozzáférés, azok módosítása, a járművek irányításának, működésének befolyásolása szakértői feladatokat indukálhat, ezen tevékenységek a vizsgálati oldalon jelennek meg. A szakértői munka végrehajtásához szükséges lehet személyek mint információforrások igénybevétele. HUMINT esetén az információhoz, dokumentumokhoz való hozzáférés mindig személyeken keresztül történik. Polgári alkalmazásban főként az üzleti hírszerzéshez tartozik.

A járművek szerviz- és műszaki dokumentációinak, tudományos közleményeknek, szabványoknak és egyéb leírásoknak az elérésére nyílt forrású információszerzés (OSINT) is alkalmazható. A mindenki számára elérhető információk, az interneten megtalálható anyagok tartoznak ide. Ezek az információk nehezen feldolgozhatók, tévesek vagy hiányosak lehetnek, hitelességük megkérdőjelezhető, nehezen ellenőrizhető. A járművek digitalizációjának gyors üteme miatt ezen információk naprakészége sem garantálható.

A járművek digitális szakértői vizsgálataihoz kapcsolódóan az adat- és információigény teljesítésének eszköze a technikai hírszerzés (TECHINT), amely a járművek, a közlekedési rendszer komponenseinek közvetlen vizsgálatát és a hozzáférhető információk feldolgozását jelenti. A SIGINT, az IMINT, a MASINT és a CYBINT megoldást csekély alkalmazási hatékonysága és a magas erőforrás-ráfordítás miatt jellemzően nem használják (5.1. táblázat).

Katonai alkalmazásban az emberi erőforrásokkal folytatott információ- és hírszerzési tevékenységet a nyílt, legális és az ügynöki, fedett hírszerzés jelenti. „A nyílt, legális pozícióból folytatott információ és hírszerzést alapvetően diplomáciai keretek között, valamint a katonai missziók hír- és információs szerző támogatását ellátó hírszerző elemekkel (a katonai hírszerzéshez tartozó NIC – *National Intelligence Cell*, NIST – *National Intelligence Support Team*) folytatott hírszerzés alkotja.”³

Rádióelektronikai felderítés esetén passzív eszközökkel az elektromágneses hullámokat kibocsátó rendszerek felfedése és lehallgatása történik. Járművekhez kapcsolódóan a kommunikációs csatornák felfedésével és hallgatásával érhetők el a digitális adatok (például távirányított vagy autonóm eszközök adatcsatornáinak telemetriai adatai).

³ BÉRES 2014: 122.

5.1. táblázat. Modern járművek vizsgálata esetén alkalmazható információszerzési területek polgári és katonai alkalmazásban

Polgári alkalmazás		Katonai alkalmazás	
<i>HUMINT</i>	X	<i>HUMINT</i>	X
<i>SIGINT</i>		<i>SIGINT</i>	X
<i>OSINT</i>	X	<i>OSINT</i>	X
<i>IMINT</i>		<i>IMINT</i>	X
<i>MASINT</i>		<i>MASINT</i>	X
<i>TECHINT</i>	X	<i>TECHINT</i>	X
<i>CYBINT</i>		<i>CYBINT</i>	X

Forrás: a szerzők szerkesztése

Nyílt forrású információszerzés polgári felhasználáshoz hasonlóan katonai alkalmazásban is használható hasonló feldolgozási nehézségekkel és problémákkal.

A képfelderítés vonatkozásában a térinformatikai felderítéssel összevont műholdas vagy légi felderítés használatával gyűjthető információ a műveleti területen megtalálható modern vagy autonóm járművekről. A műveleti területről, annak objektumairól, a járművekről, eszközökről, készült fényképfelvételek nyújthatnak plusz információt.

Azon alapinformációk megszerzéséhez, amelyek egy jármű hollétére, annak idejére, a jelenlét okaira vonatkoznak, a rádióelektronikai felderítés és a képfelderítés mellett jól alkalmazható a mérés- és jelmeghatározó felderítés (MASINT). Az azonosítás szenzorok segítségével, a kibocsátott jelek alapján történik.

A jármű a benne található nyomok kinyerése, valamint a működésére vonatkozó információk megszerzése érdekében közvetlen vizsgálat alá vonható a technikai hírszerzés (TECHINT) módszerei alkalmazásával. A modern járművekben található digitális adatokhoz történő hozzáférés ugyanis főként a technikai hírszerzés eszközrendszerével – annak járművekhez illeszkedően kialakított módszertanát és technikáit alkalmazva – közvetlenül történik, vezetékes vagy vezeték nélküli csatlakozás, illetve az adathordozóhoz történő közvetlen csatlakozás által.

Annak függvényében, hogy a járműhöz vagy valamely adattárolójához milyen módon és céllal férünk hozzá, megkülönböztethetők az egyes vizsgálati eljárások:

- ép, működőképes lefoglalt, zsákmányolt vagy más úton megszerzett eszköz/adattároló vizsgálata;
- működés vagy üzem közben lefoglalt, zsákmányolt vagy más úton megszerzett eszköz/adattároló vizsgálata;
- működés vagy üzem közben ideiglenesen vizsgálat alá vont eszköz vizsgálata;
- sérült, meghibásodott, megsemmisített eszköz vagy adattárolójának vizsgálata.

A kiberhírszerzés (CYBINT) számítógépes hálózatokban tárolt információk megszerzésére irányul. A modern járművek és a magas automatizáltságot támogató közlekedési rendszerek (*Intelligent Transport Systems, ITS; Cooperative Intelligent Transport Systems, C-ITS*) vizsgálatához tartozik mind a nyílt és zárt számítógépes hálózatokban védett információk megszerzése, mind a hálózatok által kisugárzott jelekből folytatott adatszerzés.⁴

A járművek adatkinyerési módszerei

A magas automatizáltságu, fejlett kommunikációs és adatfeldolgozási képességekkel rendelkező járművek adataihoz történő elemzési és hozzáférési módok két-két csoportba sorolhatók *live*, élő és *post mortem*, vagyis utólagos vizsgálat.

A *live forensics* vizsgálat esetén a jármű azonnali, működés közbeni vizsgálata történik meg. Ilyen vizsgálatra katonai műveletekben, hírszerzési tevékenység során vagy terrorcselekmény elkövetésének nyomozati tevékenysége során lehet szükség. Az ilyen vizsgálatok előnyei közé tartozik az „illékony” adatok (például a jármű memóriájában vagy vezérlőegységeiben ideiglenesen megtalálható adatok) megszerzése, a gyors elemzés és értékelés lehetősége. Az utólagos vizsgálat során a vizsgálandó jármű, eszköz, rendszer kikapcsolt (esetlegesen üzembe helyezhető) állapotban van.

A hozzáférés módja szerint megkülönböztetünk *online* és *offline* hozzáférést. *Online* hozzáférés során a jármű megbontása, szétszerelése nélkül történik az adatgyűjtő vagy vizsgálóeszköz, szoftver csatlakoztatása. *Offline* hozzáférés esetén olyan hardveres megoldások, csatlakozáskialakítás szükséges, amely szükségessé teheti a jármű megbontását, az egyes alkatrészek eltávolítását, az adathordozó

⁴ BÉRES 2014; CLARK 2010.

elemek (például integrált áramkörök, elektronikus vezérlőegységek) közvetlen elérését, a feszültség szintek mérését.

SIGINT, IMINT, MASINT, TECHINT, CYBINT esetén lehetőség van a *live* vizsgálatra, ilyenkor a működő rendszer adatainak *online* megszerzése és gyors elemzés történik. Ez az eljárás lehetőséget biztosít az illékony – például memóriában található – adatok vagy a kommunikációs csatornán átvitt információk megismerésére.

Utólagos vizsgálat esetén az adatokhoz történő hozzáférés történhet *online* és *offline* módon egyaránt, az ép vagy nem működő, sérült, meghibásodott vagy megsemmisített eszközön vagy annak adathordozóján. Ebben az esetben az élő vizsgálat ellentétben az illékony memóriában található adatok visszaállítása már nem lehetséges.

A járművekben hozzáférhető adatok és kihívások

A járművekhez kapcsolódó adatkinyerési módok, hozzáférési megoldások esetén az egyes adatforrásokból eltérő mennyiségű, minőségű és a katonai műveletek vagy a szakértői vizsgálatok szempontjából releváns információ érhető el, nyerhető ki. A járművekre, vezérlőegységekre vonatkozó általános információk lehetnek:

- a jármű gyártója;
- motorszám/kód;
- hengerűrtartalom;
- teljesítmény;
- üzemanyag;
- környezetvédelmi osztály;
- a vezérlőegység neve;
- a vezérlő egyedi azonosító típusa;
- a vezérlő egyedi azonosító száma;
- sorszáma;
- alvázszám;
- évjárat;
- a jármű típusa;
- a jármű felszereltsége.

A csatlakoztatott eszközök adatai, a navigációs adatok, a vezérlők adatai, az eseményadatok körében a járművek gyártónként és típusonként eltérők (5.1. ábra).

Audi_A6

Created:

3/11/2024 10:38:13 AM

Last Modified:

3/11/2024 2:45:27 PM

Vehicle Details

Year:

2013

Make:

Audi

Model:

Trim:

VIN:

WAUJ...

Vehicle Data

Geolocation (50)

Events (282)

Attached Devices (75)

ECUs (1)

5.1. ábra. A vizsgált járműben elérhető navigációs, esemény- és csatlakoztatott eszköz-adatok megjelenítése
Forrás: a szerzők szerkesztése

A navigációs adatok alapján például útvonalelőzmények, mentett helyek, korábbi úti célok, aktív és inaktív útvonalak térképes megjelenítése is lehetséges a kinyert adatok alapján. Ez nagymértékben hozzájárul az adatok értelmezhetőségéhez.

A jármű helyadatai a közterület nevével, idejével, hosszúsági és szélességi adataival rögzíthetők. A jármű továbbá rögzítheti saját navigációjának használatát vagy a csatlakoztatott mobileszköz lokációs információit is (5.2. ábra).

Audi_A6							
Applications			Name	Date/Time	Timestamp Type	Latitude	Longitude
Connections			TÉR		Local	47,6	6 19,1 9
Devices (74)			KÖZ		Local	47,6	9 21,1 0
Events (282)			ILKA		Local	47,6	1 22,1 6
Navigation					Local	46,6	6 20,1 9
Tracklogs			OS UTCA		Local	47,6	0 19,1 3
Locations (50)			JEN UTCA		Local	47,6	3 19,1 2
Routes			I ÚT		Local	47,6	3 19,1 4
Velocity Logs			TÉR		Local	47,6	7 19,1 2
			JNA UTCA		Local	47,6	5 19,1 5
			ITCA		Local	47,6	5 19,1 7
			ARU UTCA		Local	47,6	9 19,1 6

5.2. ábra. A járműben rögzített navigációs adatok
Forrás: a szerzők szerkesztése

Audi_A6								
Applications	Flags	Device Name	Device Type(int)	Device Type	Unique Number	Unique Number Type	Manufacturer	
^ Connections					0i	> Bluetooth Address		
Bluetooth (71)					0i	E Bluetooth Address	MAC-> Apple	
Wifi					0i	I Bluetooth Address	MAC-> Samsung	
USB					0i	1 Bluetooth Address		
^ Devices (74)					0i	7 Bluetooth Address		
^ Events (282)					0i	3 Bluetooth Address		
Call Log (197)					0i	D Bluetooth Address		
Device (85)					1i	1 Bluetooth Address	MAC-> Wingtech	
^ Navigation					1i	3 Bluetooth Address		
Tracklogs					2i	3 Bluetooth Address		
Locations (50)					2i	> Bluetooth Address		
Routes					2i	F Bluetooth Address		
Velocity Logs					2i	5 Bluetooth Address		
					2i	D Bluetooth Address		
					2i	D Bluetooth Address		
					2i	0 Bluetooth Address		

5.3. ábra. A vizsgált jármű Bluetooth-kapcsolatainak listája

Forrás: a szerzők szerkesztése

Kinyerhetők például a csatlakoztatott mobiltelefon azonosítói, annak szinkronizált adatai, a médialejátszó, az USB-meghajtók, az SD-kártyák részleges vagy teljes tartalma, vezeték nélküli hozzáférési pontok azonosító adatai stb. Az 5.3. ábrán látható, hogy a vizsgált jármű lehetséges vezeték nélküli kapcsolatai közül csak Bluetooth-kapcsolattal csatlakoztatott mobil eszközöket használtak. Amennyiben a csatlakoztatott mobil eszköz név- vagy típusadatokat is megoszt magáról, a jármű ezeket is képes tárolni, hasonlóképpen, mint az egyedi azonosítót (például IMEI, IMSI) vagy a gyártó nevét. A jármű rögzíti (5.4. ábra) a csatlakoztatott mobiltelefonról kezdeményezett vagy fogadott hívások idejét másodpercre pontosan, a telefonszámokat, illetve a telefonkönyvben szereplő nevet is (amennyiben mentett telefonszámról van szó).

Járműesemények és balesethez kapcsolódó rögzített adatok: az ajtónyitás/-zárás időbélyegei, a biztonsági öv bekapcsolása, a világítás be-/kikapcsolása, a rendszer újraindítása, a GPS-időszinkron, a sebesség, a kormányoszög, a kilométeróra-állás, a sebességváltás, az erős gyorsítás/lassítás, a vezetői figyelmeztetések stb. (5.5. ábra).

A modern, magas automatizáltságú járművek szakértői vizsgálatának eljárásához kapcsolódó kihívásainak egy része megjelenik az adatok hozzáférhetőségének és értelmezhetőségének kérdéskörében is. Komplex vizsgálatok a járművek központi egységének/fejegységének fejlesztésével, a vezérlőegységek számának és funkcióinak növekedésével, a járművek hálózati komplexitásának növelésével jelentek meg. A navigáció és a mobil eszközökkel kialakított kapcsolat révén olyan

	Start Time	Timestamp Type	Flags	Timestamp Confidence	Phone Number	Contact Name	Call Type
	2019.0 .16 15: :58	Local	In Vehicle	Medium	+3630 7		Unknown Direction
	2019.0 .06 11: :35	Local	In Vehicle	Medium	+3620 1		Unknown Direction
	2019.0 .21 14: :43	Local	In Vehicle	Medium	+3630 0		Unknown Direction
	2019.0 .04 14: :24	Local	In Vehicle	Medium	+3620 9		Unknown Direction
	2019.0 .12 16: :51	Local	In Vehicle	Medium	00	8	Unknown Direction
	2019.1 .11 12: :29	Local	In Vehicle	Medium	06		Unknown Direction
	2020.0 .03 13: :39	Local	In Vehicle	Medium	00	3	Unknown Direction
	2020.0 .27 11: :32	Local	In Vehicle	Medium	+3620 0		Unknown Direction
	2020.0 .21 16: :43	Local	In Vehicle	Medium	+3620 9		Unknown Direction
	2020.0 .27 15: :29	Local	In Vehicle	Medium	+3620 2		Unknown Direction
	2020.1 .13 07: :17	Local	In Vehicle	Medium	+3620 2		Unknown Direction
	2020.1 .24 08: :22	Local	In Vehicle	Medium	+9725 97		Unknown Direction
	2020.1 .10 08: :48	Local	In Vehicle	Medium	+3620 2		Unknown Direction
	2020.1 .16 11: :13	Local	In Vehicle	Medium	00		Unknown Direction
	2021.0 .19 14: :55	Local	In Vehicle	Medium	00	1	Unknown Direction
	2021.0 .19 15: :47	Local	In Vehicle	Medium	+3620 2		Unknown Direction

5.4. ábra. A járműben tárolt hívásadatok megjelenítése szakértői vizsgálat során

Forrás: a szerzők szerkesztése

mennyiségű és minőségű információ jelent meg az autókban, amely egyre kiemeltebb jelentőséggel bír a szakértői vizsgálatok elvégzése során. Komplex tudás és azt alkalmazni tudó munkaerő szükséges a vizsgálatok elvégzéséhez, ami gyakorlati ismeretek átadását is jelenti a képzések során. Magas szintű járműtechnológiai tudás mellett olyan szakértői eszközökre és azok ismeretére van szükség, amelyek az általános digitális forenzikus vizsgálatok esetén nem szükségesek, és nem állnak rendelkezésre. A nagy mennyiségű és a jármű különböző egységeiben található adatok kinyerése és azok korrelációja, a központosított időszinkronizáció hiánya, az eseménylánc végigkövetése, vezetése, az adatokból felismerhető mintázatok felismerése mind-mind nagy szakértői tapasztalatot igényel.⁵ A vizsgálatok végrehajtásának időprése, az adatok kinyerése és elemzése mellett a jármű folyamatos adatgyűjtése és a tárolt adatok gyors felülírási ciklusa is nehezíti az eljárást. Az adatok sértetlenségének és hitelességének biztosítása a felügyeleti lánc (*Chain of Custody*) segítségével a műveleti területen nagy kihívást jelent.

A fentiek mellett figyelembe kell venni továbbá azt is, hogy a külső környezeti feltételek műveleti területen ritkán teremtenek ideális körülményeket a vizsgálatok zavarmentes lebonyolításához. A kellemetlen meteorológiai viszonyok gyakran extrém jellemzőket mutathatnak. A jövőben számolni kell azzal, hogy az éghajlatváltozás az időjárási extrémítások gyakoriságának növekedését és intenzitásának

⁵ RÉPÁS–NÉMEDY 2023; ROGERS–PIPER–BATES 2023.

Events (41455)	Runtime	Date/Time	Timestamp Type	Event Identifier	Event Type	Action
Device (8)		2017.03. 12:10:38	UTC	Odometer Value: 17667.5 KM (10978.4 Miles)	Odometer	Read
Door (14307)		2017.03. 12:11:00	UTC	Odometer Value: 17667.5 KM (10978.4 Miles)	Odometer	Read
Ignition (21260)		2017.03. 12:11:13	UTC	Odometer Value: 17667.5 KM (10978.4 Miles)	Odometer	Read
Time (4700)		2017.03. 12:13:55	UTC	Vehicle Ignition Locked	Ignition	Lock
Odometer (1179)		2017.03. 12:13:58	UTC	Front Right Door Open	Door	Open
System Log (1)		2017.03. 12:14:00	UTC	Time update from Instrument Cluster: 2017-03-28 12:11	Time	Update

5.5. ábra. A jármű működési eseményeinek rögzítése

Forrás: a szerzők szerkesztése

erősödését hozza, ami sok más mellett negatívan befolyásolja a vizsgálati eljárásban felhasznált technikai eszközök alkalmazási spektrumát.⁶

A fejlett *anti-forensic* megoldások (amelyek tulajdonképpen ellenintézkedések a vizsgálat lefolytatása ellen, fő céljuk a bizonyítékok megszerzésének megakadályozása)⁷ alkalmazásának járművekben való elterjedése különösen a katonai műveletekben alkalmazott járművek vizsgálatát nehezíti meg, a polgári felhasználású járművek esetén ilyen megoldások megjelenésére még várni kell.

A modern járművek szakértői vizsgálata vizsgálóeszközökhöz kapcsolódó kihívásainak fenti általános nehézségei kapcsán azonban a járművek digitális szakértői vizsgálata messze túlmutat a jelenleg rendelkezésre álló módszertanokon, kompetenciákon, eszközökön.⁸ A szűkös vizsgálati megoldások és a rendelkezésre álló eszközkészlet gyakran lehetetlenné teszi komplex vizsgálatok elvégzését. A kompatibilitási problémák mellett a járművek típusa, évjárata vagy a vezérlőegységek gyártójának különbözősége miatt is megghiúsulhatnak vizsgálatok, mert az adatokhoz történő hozzáférésre ezek miatt nincs mód. A járműgyártók üzleti érdekeiket védve nem biztosítanak hozzáférést a fejegységek és a vezérlőegységek működéséhez, adattárolási struktúrájához, forráskódjához, ezért sok esetben a kinyert adatok értelmezése válik lehetetlenné.

⁶ PADÁNYI 2022.

⁷ JAIN–CHHABRA 2014; GARFINKEL 2007.

⁸ STANDER–BARNARD 2017.

Összefoglalás

A modern járművek forenzikus vizsgálataihoz, a járművekből történő információkinyeréshez különféle módszerek, eszközök és technikák szükségesek, amelyek alapját a digitális forenzikus vizsgálati eljárások képezik, azonban a járművekhez kapcsolódó vizsgálat, eszközök és eljárások kihívásai ezen túlmutatnak, ezek specifikus kiegészítése és módosítása szükséges. Korábbi publikációinkban ezt már igazoltuk.⁹ Jelen tanulmányban meghatároztuk azon információgyűjtési eljárásokat, amelyek műveleti területen, illetve szakértői vizsgálatok esetén alkalmazhatók, továbbá részleteztük a járművekben elérhető adatok hozzáférési módjait, kihívásait és lehetőségeit.

A járművek szakértői vizsgálati lehetőségeinek elemzése és gyakorlati végrehajtása alapján, a jármű kommunikációs és adattároló megoldásait figyelembe véve megállapítható, hogy a legbősegebb adatforrást a jármű központi egysége/fejegysége, valamint balesetekhez kapcsolódóan az Egységes Digitális Rádiótávközlő Rendszer (EDR) jelenti. *Online és offline* hozzáférés esetén vezetékes és vezeték nélküli módon is van lehetőség a jármű adataihoz történő hozzáférésre, adatainak kinyerésére, azok élő vagy utólagos elemzésére.

Felhasznált irodalom

- Autopro.hu/R.K.E. (2024): A Mercedes élre tör az önvezető autók piacán. *Autopro.hu*, 2024. február 7. Online: <https://autopro.hu/gyartok/a-mercedes-elre-tor-az-onvezeto-autok-piacan/1047211>
- BEREK Lajos – BEREK Tamás – RÉPÁS József (2023): A komplex vagyonvédelem értelmezése a modern közlekedési és az autonóm harctéri járművek vonatkozásában. In GÖCZE István – PADÁNYI József (szerk.): *Húsz év a katonai műszaki tudományok szolgálatában. A katonai műszaki tudományok tudományág időszzerű kérdései, aktuális tudományos kutatási eredményei. Oktatói kötet*. Budapest: Ludovika, 11–28.
- BEREK Tamás – RÉPÁS József (2024): Az autonóm harctéri és közlekedési járművek forenzikus vizsgálatának lehetőségei és kihívásai. In GÖCZE István – PADÁNYI József (szerk.): *Szemelvények a katonai műszaki tudományok eredményeiből IV. Hallgatói kötet*. Budapest: Ludovika, 7–20.
- BÉRES János (2014): A hírszerzés feladatrendszere. In DOBÁK Imre (szerk.): *A nemzetbiztonság általános elmélete*. Budapest: Nemzeti Közszerződési Egyetem, 117–128.
- CLARK, Robert M. (2010): *Intelligence Analysis: A Target-Centric Approach*. Washington, DC: CQ Press.
- GÁSPÁR Péter – NÉMETH Balázs – BOKOR József (2019): *Járműűrnyitás*. Budapest: Akadémiai. Online: <https://doi.org/10.1556/9789634543282>

⁹ BEREK T. – RÉPÁS 2024.

- JAIN, Anu – CHHABRA, Guralp Singh (2014): Anti-Forensics Techniques: An Analytical Review. In *Seventh International Conference on Contemporary Computing (IC3)*. Noida: IEEE, 412–418. Online: <https://doi.org/10.1109/IC3.2014.6897209>
- PADÁNYI József (2022): *Kihívások, kockázatok, válaszok. Az éghajlatváltozás okozta kihívások és azok hatása a katonai erőre*. Budapest: Ludovika.
- RÉPÁS, József (2023): Definition of Forensic Methodologies for Autonomous Vehicles. *Hadmérnök*, 18(1), 125–141. Online: <https://doi.org/10.32567/hm.2023.1.9>
- RÉPÁS József – NÉMEDY László (2023): Modern járművek kiberbiztonsága, biztonsági követelményei a szakértői vizsgálatok céljával és lehetőségeivel összefüggésben. In BORZA Veronika et al. (szerk.): *Régi és új kihívások az igazságügyi szakértői munkában*. Budapest: Nemzetbiztonsági Szakszolgálat, 87–129.
- ROGERS, Marcus – PIPER, Megan – BATES, Sienna (2023): A Brief History of Digital Forensics and Digital Evidence. In HOUCK, Max M. (szerk.): *Encyclopedia of Forensic Sciences I*. Amsterdam: Elsevier, 9–18. Online: <https://doi.org/10.1016/b978-0-12-823677-2.00029-5>
- SIMON Zsolt (2024): Öncezető autókat tesztelhet Peking utcáin a Mercedes-Benz. *Villanyautósok*, 2024. augusztus 8. Online: <https://villanyautosok.hu/2024/08/08/onvezeto-autokat-tesztelhet-peking-utcain-a-mercedes-benz/>
- SIMSON, Garfinkel (2007): Anti-forensics: Techniques, Detection and Countermeasures. In ARMISTEAD, Leigh (szerk.): *ICIW 2007. 2nd International Conference on i-Warfare and Security*. Reading: Academic Conferences Limited, 77–84. Online: <https://simson.net/ref/2007/iciw07-cd.pdf>
- STANDER, Adrie – BARNARD, Hanlé (2017): *Digital Forensics and Electronic Evidence*. Online: www.udemy.com/course/digital-forensics-and-electronic-evidence/
- TOKODY Dániel et al. (2018): Kiberbiztonság az autóiparban. *Bánki Közlemények*, 1(3), 71–77. Online: <http://bk.bgk.uni-obuda.hu/index.php/BK/article/view/79>

