Mérnöki Szimpózium a Bánkiban
(ESB 2022)
http://bgk.uni-obuda.hu/esb/

Modern járművek, mint adatforrások az utólagos szakértői vizsgálatokban

Modern vehicles as data sources in the digital forensics examinations

[1]Pogány Viktor, [2]Répás József, Schmidt Miklós

[1]Alverad Technology Focus Kft. Budapest, Magyarország, pogany.viktor@alverad.hu
[2]Nemzeti Közszolgálati Egyetem. Budapest, Magyarország, repas.jozsef@uni-nke.hu

Összefoglalás

A mai modern, komplex vezetéstámogató funkcióval rendelkező, magas automatizáltságú és egyre inkább önvezetővé váló járművek széleskörű elterjedésével, az utólagos szakértői vizsgálatok (forensics vizsgálatok) elvégzéséhez egyre szélesebb körben állnak majd rendelkezésre információk. Ezek az információk rendelkezésre állhatnak a járművekben, egy vagy több vezérlő egységben, a járművön kívül, akár több helyszínen és szolgáltatónál, amelyekhez a hozzáférés új kihívásokat jelent a vizsgálatot elvégző szakértők számára.

Kulcs szavak: Szakértői vizsgálat, forensics, modern járművek, önvezető autó

Abstract

With the widespread of today's modern, highly automated, and increasingly self-driving vehicles with more and more driving support functions, more and more information will be available to carry out subsequent expert examinations (forensic examinations). This information may be available in the vehicles, in one or more control units, outside the vehicle, or even at multiple locations and providers; access to these data presents new challenges for the experts conducting the investigation.

Keywords: Forensics examination, modern car, autonomous vehicle

1 Bevezetés

A járművek összekapcsoltsága, az új szolgáltatások és lehetőségek több adatforrást eredményeznek, azonban az adatokhoz való hozzáférés, azok kinyerése egyre összetettebb folyamatokat és módszereket igényelnek. A jövő kooperatív intelligens közlekedési rendszereiben (C-ITS - Cooperative Intelligent Transport Systems) mind a járművekről, a közlekedés részvevőiről, a környezeti és pálya elemekről egyaránt elérhetőek lesznek olyan adatok, amelyek megfelelő kontextusba helyezésével egy szakértői vizsgálat céljainak megfelelő információkat jelenthetnek. Egyre kevesebb olyan tevékenység képzelhető el, ami ne lenne valamilyen IT eszközzel, digitális elemmel támogatva, vagy azzal végrehajtva. Igaz ez a bűncselekmények elkövetésére is. Szinte minden bűncselekményhez kapcsolódik valamilyen digitális eszköz (például számítógép, vagy mobil telefon), az esetek kb. 80 %-ában használnak valamilyen járművet az elkövetés során [13]. Napjaink járművei is számos olyan adatot tartalmaznak -melyekre az átlag felhasználó nem is

gondolna - ami egy balesetben, bűncselekmény vizsgálatakor felhasználhatóak. Az ilyen adatok mennyisége folyamatosan növekszik, a minősége egyre javul és utólagos felhasználhatósága hatékonyabbá válik. A járművek vagy a járművekhez kapcsolódó adatok hatósági vagy jogi eljárásbeli vizsgálata során a cél a releváns múlt megállapítása, annak egyértelmű meghatározása, hogy mi történt, még azokban az esetekben is, amelyek nem megismételhetőek.

2 Utólagos szakértői vizsgálat – Digital Forensics vizsgálat

A jogi eljárások fejlődése, a perbeli képviselet lehetőségeinek változása lehetővé tette, hogy a felek igazolhassák, bizonyíthassák az „igazukat". Ennek egyik módja a bizonyítékok szakértő általi feldolgozása, elemzése, melynek eredményéről állásfoglalást készít. Tanulmányunk hatókörébe a Digital Forensics vizsgálat és annak egy fejlődőben lévő új területe a járművekhez kapcsolódó vizsgálat tartozik bele. Az ilyen vizsgálatok elvégzése felhatalmazáshoz kötött, feladata a digitális adatok azonosításának, gyűjtésének, feldolgozásának, elemzésének és riportolásának gyakorlata. Olyan technikák és eszközök gyűjteménye, amelyek segítségével a vizsgálati eljárás céljának megfelelő információk előállíthatóvá válnak. Ilyen vizsgálati cél lehet:

- a járművek által elszenvedett vagy okozott közlekedési balesetek utólagos vizsgálata,
- a jármű érintettségével, közreműködésével elkövetett bűncselekmények vizsgálata,
- személyek vagy szállítmányok nyomonkövetése.

3 A járművekben végzett szakértői vizsgálatok és adatok

A járművekhez kapcsolódó, utólagos szakértői vizsgálatok a járművek folyamatos fejlődése (gyártók egyre inkább elmozdulnak a funkcióktól a szolgáltatások irányába), szoftver orientálttá való alakulása, a belső struktúra változása okán új eszközöket, módszereket és folyamatokat igényel. További vizsgálatot igényel, hogy milyen technológiák, eszközök és adatok állnak rendelkezésre és alkalmasak bizonyítékként való felhasználásra. Függetlenül attól, hogy milyen egység és milyen adattárolási módot alkalmaz a gyártó az egyes járművekben, a nyomok sértetlensége a teljes vizsgálati folyamatban kiemelten fontos. A balesetek, vagy egyéb járművel kapcsolatos események vizsgálata során több belső adatforrást, a bennük tárolt adatokat is figyelembe kell venni.

3.1 Eseményadat-rögzítő és adatai

Balesetek körülményeinek vizsgálatához elsődleges adatforrás a napjainkban, az új járművekbe kötelezően beépített „fekete doboz" az eseményadat-rögzítő, az EDR – Event Data Recorder. Az ilyen eszközök alkalmazásának célja, az (EU) 2022/545 számú rendelete alapján „az, hogy röviddel ütközés előtt, ütközéskor és közvetlenül az ütközést követően az ütközés szempontjából kritikus adatokat és információkat rögzítse és tárolja annak érdekében, hogy a balesetekkel kapcsolatban pontosabb, részletesebb adatok álljanak rendelkezésre".

Az eseményadat-rögzítők tehát olyan eszközök, amelyek rögzítik a járművek műszaki paramétereit, jellemzően baleset vagy ütközésközeli esemény előtt, közben és után. Személygépjárművek, SUV-k esetén ezeket az adatokat a légzsák vezérlő (Air Bag Control Module - ACM) tartalmazza. Az eseményt az EDR általában a jármű túlzott lassulásával detektálja, ehhez elég egy erős fékezés is, ilyen esetben nem mindig következik be baleset. Tehergépjárművek esetén a motorvezérlő egységben (Engine Control Module - ECM) találhatóak. Az ECM szabályozza a motor teljesítményt, a károsanyag-kibocsátást az üzemanyag-felhasználást stb. és rögzíti a biztonsággal összefüggő adatokat is [2][4][12].

Az EDR által rögzített adatok folyamatosan frissülnek és az ideiglenes memóriában tárolódnak a légzsákok kioldásáig, melynek hatására adatok az állandó memóriába kerülnek, amelyből

visszakereshető marad [8]. Anonimizált módon tartalmazza a jármű sebességét, a motor fordulatszámát a baleset időpontjában, a fékezési információkat, a jármű pozícióját és dőlését az úton, a jármű összes biztonsági rendszerének állapotát és aktiválási sebességét, a járműbe épített eCall rendszer jelzését, a fék aktiválását és a releváns bemeneti jellemzőit a fedélzeti aktív biztonsági és balesetelhárító rendszereknek. A rendszer utasbiztonsághoz kapcsolódóan is gyűjt adatokat például a biztonsági öv, légzsákok státusza. Ezeket az információkat egyre gyakrabban használják fel tárgyi bizonyítékok kiegészítésére baleset rekonstruálása érdekében [2][4][7].

Az EDR-ben tárolt eseményadatokhoz történő hozzáféréshez, kinyerésre azonban nem állnak rendelkezésre szabványosított kommunikációs protokollok. Jelenleg a járműgyártók adnak tájékoztatást arról, hogy milyen módon férhetőek hozzá és értelmezhetőek ezen adatok. A lekérdezése az alkalmazott módszerek licensszel védettek. Meghatározott gyártók (például: GM, Ford, Chrysler és bizonyos partnerei) és a Bosch által használhatóak. A Hexadecimális Fordító eszközöket (HTT- Hex To Text) az EDR gyártók készítik el. A Bosch 2008. óta gyártja a Crash Data Retrieval Tool (CDR) eszközt, ami az egyetlen olyan nyilvánosan elérhető, harmadik féltől származó (nem gyártói) eszköz, amely képes az EDR-ekben tárolt adatok kinyerésére és értelmezésére.

3.2 Jármű központi egység, fejegység és adatai

Bár az EDR-ek fontos adatforrásként jelennek meg egy esemény, baleset körülményeinek a szakértői vizsgálatakor, a vezérlőegységek számának növekedése, az egyre inkább önvezetővé váló járművek fejlődésével párosulva, egyre inkább szerepet kapnak a jármű központi egységek (fejegységek), telematikai-infotainment rendszerek és a bennük tárolt adatok, számos lehetőséget és kihívást jelentve a vizsgálatot elvégző szakembereknek. Az elérhető adatok mennyisége és a „választék", az adatok köre folyamatosan növekszik és egyre fontosabbá válnak. A vizsgálatok folyamatára és eredményeire egyre nagyobb hatást gyakorolnak, mivel az összes gyártó beépít már valamilyen szintű beágyazott rendszert új járműveibe, melyek egyre több járművön belüli és azon kívüli kapcsolattal fognak rendelkezni [3]. Ahogy a magas automatizáltságú és egyre inkább önvezető járművek aránya a napi közlekedésben növekszik, úgy fog emelkedni az ellenük elkövetett bűncselekmények, vagy az olyan balesetek száma, mely során az ilyen jármű kerül konfliktusba, vagy ütközik emberi vezető által irányított autóval. Egyre gyakoribbá válhatnak az járműrendszerek elleni támadások, valamint a járművek távoli táveltérítése, irányítása is. Az ilyen bűncselekmények során keletkező adatok megszerzése és elemzése kulcsfontosságú lesz a a szakértők számára[14].

A központi egységekben tárolt adatok mennyisége és forrása gyártónként eltérő, esetenként a járműmodellek vagy gyártási évek között is lehetnek különbségek. Tárolásra kerülnek a járműben található vezérlő egységek ECU-k azonosító adatai (például sorozatszám, frissítési és újraindítási információk, szoftver verzió, gyártási számok), vagy a járműhöz vezetékes vagy vezeték nélküli módon csatlakoztatott eszközök adatai (például USB eszköz, SD-kártya, mobiltelefon stb.), navigációs adatok (például útvonal, korábbi úti célok stb.), eszközinformációk és a jármű működési eseményei (például indítás, leállítás, sebességváltás, gyorsítás, fékezés stb.).

A csatlakoztatott eszközről olyan adatokat tárol a rendszer, mint például az eszköz neve, gyártója, interfész típusa és az eszköz egyedi száma vagy MAC-címe. A GPS és a jármű működési eseményadatok tartalmazzák a navidágiós adatokat minden rögzített eseményhez, valamint a jármű pontos helyzetét. Részletes információk ismerhetőek meg az aktív és inaktív útvonalakról, mentett helyekről, korábbi úticélokról, ezekhez megőrzésre kerül dátum, idő, város- és utcanév is. Ezek az információk egy szakértői vizsgálat során felhasználhatóak egy esemény vagy eseménysorozat idővonalának létrehozásához, helyszíneinek és az érintett személyek meghatározásához [6][11].

3.3 Key Fobs - távirányítók

Egyes források szerint a járművek távirányítói is egyre több digitális bizonyítékot tartalmaznak, potenciális adatforrássá válhatnak. Ezek a kulcsrendszerek a vizsgálathoz kapcsolódóan tárolhatnak hasznos információt, mint például a jármű azonosítót, kulcs ID-t, idő- és dátumbélyegzőket, kilométeróra állást, vagy éppen a kulcs utolsó használati időpontját [3].

3.4 Egyéb adatforrások

A jármű által érzékelt, szerzett, rögzített információk mellett a közlekedési rendszerek fejlődésével egyre több külső adatforrás is elérhetővé válik/válhat a szakértői vizsgálatok elvégzéséhez. A kooperatív intelligens közlekedési rendszerek által a környezeti elemekből, pályaelemekből is rendelkezésre állnak információk, amelyek az adott üzemeltető, hatóság által válnak hozzáférhetővé, vizsgálhatóvá. A különböző cloud megoldások, azok szolgáltatói, a járművekkel kapcsolatban álló szerverek és alkalmazások naplói kiegészítő információt jelenthetnek az egyes vizsgálatokhoz. A különböző telekommunikációs rendszer és szolgáltatói naplók napjainkban is elérhetőek a jogosult szervezetek számára, ezek szerepe a járművek önálló kommunikációs csatornáinak elterjedésével még hangsúlyosabbá válnak a jövőben. Bár ezek a járművön kívüli, külső adatforrások javítják a vizsgálatok teljesítményét, hatékonyságát, az adatok hozzáférhetősége, begyűjtési lehetőségei, tulajdonjoga új kihívásokat jelentenek. Jelen tanulmány azonban nem terjed ki ezen kihívások részletes vizsgálatára [10].

4 Szakértői vizsgálatok adatkinyerési lehetőségei

A járművek központi egységeiben található adatok kinyerése elvégezhető manuális módszerrel, az infotainment felhasználói felületén manuálisan navigálva, az információk a jármű kijelzőjén jelennek meg. Logikai módszernél a vezérlő egységek memóriájából vagy azok egy részéből nyerhetőek ki a jármű által generált, érzékelt, vagy a felhasználó által létrehozott adatok és fájlok, függetlenül attól, hogy aktív vagy törölt adatokról van szó. Nem invazív módszer esetén az ECU adataihoz való hozzáférés, azok kinyerése anélkül biztosítható, hogy fizikailag hozzá kellene férni a vezérlő egységhez, meg kellene bontani a jármű műszerfalát, vagy az eszköz burkolatát. Például szabványos csatlakozón keresztül, OBD-II, vagy USB port.

Invazív módszer alkalmazása esetén az ECU adataihoz, az 1. ábrán látható módon, a jármű műszerfalának megbontásával az egység szétszerelésével juthatunk hozzá.

Az adatok kinyerésére több megoldás alkalmazható, J-tag módszer, „chip-off" eljárás, microRead módszer. A J-tag módszer esetén a vezérlő egységen található szervízpontok, kivezetések, csatlakozók felhasználásával, azokat a vizsgáló számítógéppel összekapcsolva válnak kinyerhetővé a tárolt adatok. Chip-off eljárás esetén a memóriachip eltávolításra kerül a vezérlőegységből, annak adattartalma beolvasásra kerül, az elemzés elvégzéséhez.

MicroRead módszer alkalmazása során a memória áramkör tokjának eltávolítása után, nagy teljesítményű mikroszkóppal történik a vizsgálat ami fizikai képet ad a memóriáról, annak működéséről [6][8].

A járművek központi egységéből kinyert, letöltött bináris kép elemzésével a szakérői vizsgálat során olyan adatok válnak hozzáférhetővé, melynek elemzésével meghatározhatóak a vizsgálat céljához kapcsolódó kérdések, például a jármű haladási útvonala, a járművezető személye, a megtörtént események idővonala, helyszínek stb. Különböző személyek összekapcsolhatóak lehetnek a járművel egy adott helyen és időpontban. Lehetségessé válik annak meghatározása, hogy mely helyszínen és időpontban szálltak be utasok a járműbe vagy szálltak ki a járműből [6][11].

1. ábra Járműközponti egység [1][5]

5 Konklúzió

A digitális lábnyom, egyik meghatározása szerint „azon digitális adatok, információk összessége, amelyeket a különböző online és digitális tevékenységünk révén hagyunk magunk után életünk folyamán”[9]. Ez tartalmazza a közösségi média platformokon megosztott tevékenységeket, a levelezésünket, interneten elérhető fotóinkat eszközeink azonosítóit, amiket felismernek és elraktároznak a különböző szerverek. Digitális nyomaink körének nagy léptékű bővülését a számítógépek után a mobiltelefonok és használata által generált adatmennyiség jelentette. A szerzők véleménye szerint új mérföldkövet a modern és egyre inkább önvezetővé váló járművek jelentik, amelyek olyan mennyiségű és minőségű adatokat fognak tartalmazni, amelyek a felhasználói tevékenységek és viselkedés még pontosabb követhetőségét és elemezhetőségét teszik lehetővé. Ezek a lehetőségek egy szakértői vizsgálati eljárásban mindenképpen előnyt jelentenek, lehetővé teszik megalapozott vizsgálatok elvégzését a tanulmányban ismertetett adatforrások felhasználásával.

Köszönetnyilvánítás

A kutatás az Európai Unió támogatásával valósult meg, az RRF-2.3.1-21-2022-00004 azonosítójú, Mesterséges Intelligencia Nemzeti Laboratórium projekt keretében.

A szerzők külön szeretnének köszönetet mondani az Alverad Technology Focus Kft. ügyvezetőjének és munkatársainak a kutatási munkához nyújtott támogatásukért.

6 Hivatkozások

[1] Alpine (2022). https://www.alpine.hu/fileadmin/_productdb/imagecache/480x360_iLX-F905D_Alpine-Halo-9-sound-setting.jpg, (2022.11.10.)

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/2144 RENDELETE

[3] Bates, Eoin A. (2019). Digital Vehicle Forensics Forrás: https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf, (2021.10.22.)

[4] Event Data Recorder (2022). https://squarell.com/solutions/event-data-recorder-edr, (2022.10.15.)

[5] Ford ECU (2022). https://images.cdnrrr.com//dtr/0/0/0/0/1/0/4/8/9/0e176aab1949b8131c05f2a34bd19ceb-ford_explorer_multimedijos_kontroleris.jpg, (2022.11.10.)

[6] Selimovic, E. (2017). Forensic Investigation Of Automotive Computers by , A Capstone Project Submitted to the Faculty of Utica College

[7] Gabler, H. C., Hinch, J. A., & Steiner, J. (2008). Event Data Recorder. A Decade of Innovation.

[8] Jackson Jr, K. A. (2020). Infotainment and Telematic Systems Challenges Effecting Vehicle Forensic Law Enforcement Capabilities (Doctoral dissertation, Utica College).

[9] Quadron (2022). Mi az a digitális lábnyom és milyen veszélyeket rejt a közösségi médiában?, https://www.quadron.hu/blog-9, (2022.11.15.)

[10] Bucks (2022). Mobile Forensics, https://www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/IntroToMobileForensics.pdf, (2022.09.22.)

[11] 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

[12] Crash Response LLC (2022). Truck EDR (Black box) download and analysis, https://crashresponse.com/services/truck-edr-black-box-download-and-analysis/ (2022.11.11.)

[13] Berla (2015). Forensics, https://berla.co/12-days-of-vehicle-forensics/, (2022.10.11.)

[14] Proven Data (2022). What is Digital Forensics and Why Is It Important?, https://www.provendatarecovery.com/blog/what-is-digital-forensics/ (2022.10.20.)