

A magas automatizáltságú közlekedési járművek utólagos szakértői vizsgálatához szükséges készségek

A polgári és katonai közlekedési járművek folyamatos fejlődése, az új és egyre precízebb vezetéstámogató funkció megjelenése, a mesterséges intelligencia széles körű elterjedése a közlekedési ágazatban, a járművek komplex szenzorhálózata segítségével összegyűjtött és rendelkezésre álló nagy mennyiségű környezeti információ előrevetíti az egyre inkább önvezetővé váló közlekedési járművek megjelenését. A digitális forenzikus vizsgálatok egyik új területének tekinthető az autonómjárművek utólagos szakértői vizsgálata. A modern járművekhez kapcsolódó vizsgálati célok eléréséhez, az információk kinyeréséhez, feldolgozásához, elemzéséhez, értékeléséhez új készségek megszerzése szükséges. A tervezett tanulmányban meghatározom azon kulcsfontosságú készségelemeket, amelyek nélkülözhetetlenek az új típusú forenzikus vizsgálatok elvégzéséhez.

Kulcsszavak: forenzikus vizsgálat, önvezető járművek, szakértői vizsgálat, NICE

THE NECESSARY SKILLS FOR CONDUCTING FORENSICS EXAMINATIONS ON HIGHLY AUTOMATED TRANSPORT VEHICLES

The continuous development of civil and military transport vehicles, the appearance of new and increasingly precise driver assistance functions, the widespread use of artificial intelligence in the transport sector, and the large amount of environmental information collected and available with the help of the complex sensor network of vehicles foreshadow the emergence of transport vehicles that are becoming increasingly autonomous. One of the new areas of digital forensics testing is the forensics examination of autonomous vehicles. It is necessary to acquire new skills to achieve test goals related to modern cars, extract, process, analyse, and evaluate information. The planned study identifies key skill elements that are essential for conducting new types of forensics studies.

Keywords: digital forensics, autonomous vehicles, forensics examination, NICE

¹ Doktorandusz, Nemzeti Köszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: repas.jozsef@uni-nke.hu; ORCID ID: 0000-0002-1186-4731.

Bevezetés

A polgári és katonai közlekedési járművek folyamatos fejlődése, az egyre inkább önvezetővé váló járművek hozzájárulnak a közlekedés biztonságosabbá tételéhez, az erőforrások felhasználásának optimalizálásához, katonai műveletek során pedig az emberi erőforrás megóvásához, az új műveleti képességek kialakításához. Ahogy a járművek egyre kifinomultabbá válnak, és egyre több vezetéstámogató funkcióval rendelkeznek, egyre bonyolultabbá is válnak. Ez az összetettség megnöveli a kiberbiztonsági aggályokat, mivel a jármű szolgáltatásai és összetevői közötti kommunikáció sérülékeny lehet. A fejlett vezetéstámogató rendszerek biztosítani tudják a járművek egyes funkcióinak ellátását, vagyis lehetőség nyílik a feladatok delegálására, az automatizáltsági szint növekedésével pedig elegendő pusztán ezek felügyelete. A teljes autonómia sem polgári, sem katonai felhasználásban nem jelent még meg, jelen tanulmány írásának idején. Különböző szakértői megközelítések még mindig 5–10 éves távlatra becsülik, annak ellenére, hogy ez az időtartambecslés előfordult már 5 évvel ezelőtt is. Mivel a járművek felügyeletéhez, szükség szerinti irányításához nem szükséges a helyszínen lenni, biztonságos, gyors kommunikációs csatornán keresztül ezek a feladatok távolról elvégezhetők. Az emberi interakció azonban eltérő a jármű automatizáltságának függvényében. A szükséges technológia, a felelősségi körök vagy a következmények különbözők. A jármű által végrehajtott feladatok eltérők azok bonyolultsága, kritikussága/fontossága és kockázata szerint. A polgári közlekedésben nem mindegy, hogy a jármű utasokat vagy árut szállít, városi környezetben vagy nagy sebességgel autópályán közlekedik. Harcjármű tekintetében pedig az ellátott feladat vonatkozásában van jelentős eltérés, például anyagmozgatási vagy harci támogató, illetve harci feladatokban. A félautonóm jármű akár a kritikus döntést igénylő feladatok esetén is elvégzi/előkészíti az OODA²-ciklus, azaz az emberi döntéshozatali ciklus lépéseit, azonban az emberi tényező a ciklusban marad, a folyamat felügyelt, szükség szerint megszakítható. A digitális forenzikus vizsgálatok egyik új területének tekinthető a magas automatizáltságú, autonómmá váló járművek utólagos szakértői vizsgálata. A vizsgálati célok eléréséhez, az új technológiai környezetből történő információkinyeréshez, -feldolgozáshoz, -elemzéshez, -értékeléshez új készségek elsajátítása szükséges.

² *Observe, Orient, Decide, Act* – megfigyelés, feldolgozás, döntés, cselekvés.

Jelen tanulmányban meghatározom azon kulcsfontosságú készségelemeket, amelyek nélkülözhetetlenek az új típusú forenzikus vizsgálatok elvégzéséhez.³

Digitális forenzikus vizsgálat modern járművek esetén

A digitalizáció előrehaladtával az élet szinte minden területén szükséges vagy célszerű valamilyen digitális eszköz (például mobiltelefonok, táblagépek, számítógépek stb.) használata feladataink elvégzéséhez. Nehéz olyan területet, szakmát mondani, ahol közvetlenül vagy közvetve ne lennének jelen a digitális eszközök. A közlekedésben kiemelten igaz ez, akár polgári, akár katonai vonatkozásban nézzük, a járművek egyre komplexebb számítógép-, szerver-, tárgyakinternete- (*Internet of Things*, a továbbiakban: IoT), kommunikációs stb. rendszerként értelmezhetők. „Mivel a közlekedési rendszerek kritikus infrastruktúráknak számítanak, különösen nagy jelentőségű a magas rendelkezésre állásuk és a biztonságos működtetésük.”⁴ Fejlett, gyors, biztonságos kommunikációs csatornákon keresztül kommunikálnak egymással, a környezetükkel, a pályaelemekkel, a gyártói vagy szolgáltatói háttérrel. Szenzoraik, együttműködő szenzorhálózatuk segítségével temérdek információt gyűjtenek környezetükről és a közlekedés résztvevőiről. A (személyes) adatok védelme elsődleges feladat, ahogyan annak megállapítása is, hogy egy bekövetkezett (biztonsági) eseményhez kapcsolódóan mi, hogyan, mikor, miért, hol történt, és milyen érintettjei voltak az eseménynek: vagyis az esemény rekonstruálása, a kulcsfontosságú digitális nyomok, objektív bizonyítékok gyűjtése, visszaállítása a megállapítások alátámasztására. Korábban a járművek utólagos szakértői vizsgálata jellemzően tárgyi bizonyítékoknak (például ujjlenyomatok) és a járművek fizikai állapotának a felmérését, ellenőrzését jelentette. Mára a digitalizált járművek esetén a digitális forenzikus vizsgálat a járművekben (különböző vezérlő és adattároló elemeiben) megtalálható, helyreállítható, kinyerhető digitális nyomok elemzésével foglalkozik.⁵ Ezek a digitális nyomok lehetnek:

- a) a járműre, jármű- vagy közlekedési rendszerre vonatkozó információk;
- b) a jármű közlekedéséhez kapcsolódó működési, közlekedési paraméterek;
- c) szenzorinformációk;
- d) a járműben telepített különböző alkalmazások;

³ TÓTH-VÉG 2022; GYARMATI-SIMÓ 2021; RÉPÁS 2023; CHANDEL 2020.

⁴ BÓDI 2022; RÉPÁS et al. 2022.

⁵ HEGYI 2023.

- e) a kommunikációs csatorna adatai (például felhőalapú rendszerek, környezeti és pályához kapcsolódó adatok);
- f) a járműhöz csatlakoztatott eszközökhöz kapcsolódó információk vagy ezen eszközök adatai.

Jól látható, hogy a járművek a saját közlekedésükhöz nélkülözhetetlen információk mellett széles körben tartalmazhatnak információt környezetükről, a közeli járművekről, a járművezetőről vagy az utasokról. Ezek az információk a jövőben még nélkülözhetetlenebbek lesznek az események releváns körülményeinek tisztázása során. Ahhoz, hogy a vizsgálati célokat a szakértők, a szakemberek teljesíteni tudják, számos kihívással kell szembenéznük, amelyek kapcsolódhatnak magához a vizsgálati eljáráshoz vagy a vizsgálati eszközökhöz. Lehetnek műszaki, működési, jogi és vizsgálati kihívások is, amelyek hátráltatják a vizsgálat elvégzését, vagy növelik a vizsgálat idejét, erőforrásigényét.⁶ Ilyen például a szakértői készségek hiánya, amelyek különösen katonai műveletekhez kapcsolódó vizsgálatok esetén válhatnak kritikussá.⁷

A modern járművek szakértői vizsgálatához szükséges készségek

A különleges szakértelmet igénylő területek száma folyamatosan nő, különösen az IT-, az IoT- és egyéb digitális megoldásokat alkalmazó szférákban. A társadalmi viszonyok is egyre bonyolultabbá válnak, ami az igazságszolgáltatásban úgy jelent meg, hogy a peres, illetve a hatósági eljárások tárgyi és szerkezeti összetétele jelentős változáson ment át. Jellemzővé vált, hogy a jogi problémák más szakmákat, szakterületeket érintő előkérdéseket vetnek fel, emiatt megítélésük egyre nehezebbé válik. Ezzel párhuzamosan a bírósági eljárásokban megnőtt az igény a modern tudomány eredményeinek a bizonyítási eljárásban történő felhasználása iránt. Különösen igaz ez a műszaki vonatkozású kérdésekben, például az informatikában és a kommunikációs technológiákkal egyre inkább átszőtt közlekedésben is, ahol a járművek autonómítási szintjének növekedésével is fennmarad az igény a bekövetkezett események utólagos szakértői vizsgálatára, a szakértői tevékenység elvégzésére.

⁶ RÉPÁS–SCHMIDT 2023.

⁷ YAACOUB et al. 2021; *The Phases of Digital Forensics* [é. n.].

Az igazságügyi szakértők feladatait és kötelezettségeit, valamint az igazságügyi vizsgálatok lefolytatására irányuló jogait a nemzeti jogszabályok állapítják meg. A legtöbb ország követelményeket (oktatás, képzés és/vagy igazolás) ír elő az igazságügyi szakértőként történő elismeréshez és adott területen az igazságügyi vizsgálatok lefolytatásához. A 2016. évi XXIX. törvény az igazságügyi szakértőkről (szakértői törvény) az igazságügyi szakértői tevékenységet az alábbiak szerint határozza meg: „Jogszabályban meghatározott követelményeknek megfelelő igazságügyi szakértő, illetve az igazságügyi szakértő munkáját segítő egyéb személyek által, a kirendelő hatóság, bíróság, ügyészség, rendőrség, közjegyző, bírósági végrehajtó (a továbbiakban együtt: hatóság) kirendelése vagy megbízás alapján, e törvény által meghatározott szervezeti keretek között, jellemzően szakértői díj ellenében végzett, a hatóság eljárásaiban különleges szakértelmet igénylő tény vagy egyéb körülmény megállapítását vagy megítélését elősegítő részecselekmények összessége, így különösen a szakvéleményhez szükséges vizsgálatok elvégzése, a szakvélemény előkészítése, elkészítése és előterjesztése, valamint a hatóság kérésére annak kiegészítése és az ezekkel összefüggő valamennyi részecselekmény.”⁸ Vagyis adott szakterületen a vizsgálandó tárgy vagy helyzet szakértelmet kívánó vizsgálatát végzi az igazságügyi szakértő (vagy más néven törvénytisztelő vagy kriminalisztikai szakértő).⁹

A modern járművek igazságügyi szakértői vizsgálata az intelligens közlekedési ökoszisztémában alkalmazott eszközök és bekövetkező események vizsgálatával foglalkozó, igazságügyi szakértői terület. Az ilyen vizsgálatok magukban foglalják például a járművön belüli komponensek, mint a központi egység (*Engine Control Unit*; ECU) vagy a gyártó IT-háttérrendszerében keletkező adatok vizsgálatát, de idetartozhat a járműben utazók mobiltelefonjainak, valamint a jármű és a vele kapcsolatban álló egyéb kommunikációs és közlekedési infrastruktúra adatainak gyűjtése és elemzése is.

A szakemberek kompetenciájának támogatására a Nemzeti Szabványügyi és Technológiai Intézet (*National Institute of Standards and Technology*; a továbbiakban: NIST) által kidolgozott *National Initiative for Cybersecurity Education*¹⁰ (a továbbiakban: NICE) keretrendszer és a *European Cybersecurity Skills Framework*¹¹ (a továbbiakban: ECSF) nyújt szakterület-specifikus alapokat, vagyis a digitális forenzikus vizsgálatokat mint fő témakört illetően.

⁸ 2016. évi XXIX. törvény az igazságügyi szakértőkről.

⁹ *Igazságügyi szakértők* 2021.

¹⁰ *Nemzeti kezdeményezés a kiberbiztonsági oktatásért* – szabad fordításban.

¹¹ *Európai kiberbiztonsági készségfejlesztési keretrendszer* – szabad fordításban.

A NICE keretrendszer ismerteti az egyes munkaszerepekhez kapcsolódó szükséges feladatokat, valamint ezek elvégzéséhez szükséges tudás- és készségelemeket. Az ECSF szilárd, könnyen használható, bővíthető, elérhető, interoperábilis, szektorokon átívelő és az EU szervezeti struktúrájához illeszkedő keretrendszer, amely az európai kiberbiztonsági kultúra megerősítését célozza. A keretrendszerek fő építőköveit alapul véve meghatározhatók a modern járművekhez kapcsolódó szakértői vizsgálatok elvégzéséhez szükséges készségek. A modern járművek vizsgálata vagy az elvégzendő munka minden esetben felbontható feladatokra.

A feladat olyan tevékenység, amely szervezeti vagy jelen témakör szerint a szakértői vizsgálatokhoz kapcsolódó célok elérését szolgálja. A feladatmeghatározásnak olyannak kell lennie, hogy könnyű legyen megérteni, egyértelműen határozza meg, hogy milyen tevékenységet kell végrehajtani. A feladatmeghatározás nem vagy nem minden esetben tartalmazza a feladat célját, ez ugyanis vizsgálatonként eltérő lehet. A feladat meghatározása azt írja le, hogy milyen munkát kell elvégezni. Ez a szakértői vizsgálatok kontextusában azt jelenti, hogy definiáljuk, hogy mi lesz a vizsgálatot végző szakember konkrét, megoldandó feladata.

Mivel az önvezető járművek és a modern közlekedési rendszerek szakértői vizsgálata még egy ideig nem képezi a napi szakértői gyakorlat részét, ezért egyes feladatmeghatározások valójában hipotézisek arról, hogy milyen feladatokat fog valószínűleg ellátni ezekkel megbízott szakértő. A szakértői törvény az igazságügyi szakértő feladatát az alábbiak szerint határozza meg:

„Az igazságügyi szakértő feladata, hogy a hatóság kirendelése vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását.”

A cél annak biztosítása, hogy a vizsgálat során minden olyan digitális bizonyítékot feltárjanak, amely igazolja a vizsgált tevékenységet:

- a) természetes személyekhez kapcsolja a nyomokat;
- b) rögzíti, visszaállítja, azonosítja és megőrzi a vizsgált rendszerek állapotát, bemeneteit, kimeneteit és folyamatait;
- c) elemzi, rekonstruálja és értelmezi a digitális nyomokat;
- d) elfogulatlan, minőségi nézetből mutatja be az eredményeket, azok értelmezése nélkül.

Jelen tanulmányban nem mutatom be részletesen az önvezető járművek és a modern közlekedési rendszerek szakértői vizsgálatához kapcsolódó

feladatokat, csupán a vizsgálati lépésekhez kapcsolódó főbb feladatokat, az ECSF figyelembevételével:

- a) a vizsgálatok belső szabályainak, terveinek és eljárásainak kidolgozása;
- b) a digitális nyomok azonosítása, helyreállítása, kinyerése, dokumentálása és elemzése;
- c) a jogosulatlan és jogellenes cselekmények bizonyítékainak feltárása;
- d) a szakértői elemzések lépéseinek, megállapításainak és eredményeinek részletes dokumentálása, riportálása és bemutatása;
- e) a vizsgálati, elemzési és jelentési technikák kiválasztása és testreszabása;
- f) a digitális bizonyítékok megőrzése és védelme.¹²

Adott feladat elvégzéséhez meghatározhatóak a szükséges tudás- és készségelemek. Ezek meghatározása elősegíti a szakértői feladatok ellátásához szükséges ismeretek egységesítését, kategorizálását, meghatározását és kommunikálását.

A készség definiálható mint megfigyelhető kompetencia egy tanult motoros tevékenység végrehajtásához. A kiberbiztonsághoz szükséges készségek kevésbé támaszkodnak az eszközök fizikai manipulálására, inkább olyan eszközök, keretrendszerek, folyamatok és eljárások alkalmazására, amelyek hatással vannak egy szervezet vagy egyén kiberbiztonsági helyzetére.¹³ A készségmeghatározások az egyes feladatokhoz kapcsolódnak, amelyekben a munkát végző készségeket mutat be a feladatok végrehajtásában.

A készség egy megfigyelhető cselekvés végrehajtásának képessége. A készségmeghatározások leírhatnak egyszerű vagy összetett készségeket. Adott feladat elvégzéséhez több készségmeghatározás is szükséges lehet. Hasonlóképpen egy készség gyakorlása több feladat elvégzésére is használható. A készség meghatározások lehetnek egyszerűek (például az autó multimédia-rendszeréhez kapcsolódó Bluetooth-eszközök lekérdezése) vagy összetettek (például hipotézis felállítása arról, hogy egy kiberbűnöző hogyan tud ellenőrizetlen eszközzel kapcsolatot létesíteni az autó multimédia-rendszeréhez Bluetooth-kapcsolaton keresztül) is. A készség tehát azt írja le, hogy a szakember mire képes, a feladatmeghatározás pedig az elvégzendő munkát definiálja.¹⁴

¹² European Cybersecurity Skills Framework 2022.

¹³ NEWHOUSE et al. 2020.

¹⁴ KISS [é. n.]; SWGDE/SWGIT 2010; *Tudás - mi ez, definíció és fogalom* [é. n.]; SZEGHEGYI 2011.

*A modern járművek szakértői vizsgálatához
szükséges készségek feladatokhoz rendelése*

A fenti, digitális forenzikus vizsgálatokhoz kapcsolódóan meghatározott feladatok a modern járművek szakértői vizsgálata során is értelmezhetőek, a vizsgálat elvégzésének folyamata (azonosítás, előkészítés, digitális nyomok gyűjtése, vizsgálat, elemzés, értelmezés, dokumentálás, prezentálás) mentén. Egyes készségek az egyes feladathoz, folyamatlépéshez tartoznak, több készség azonban a teljes vizsgálat során szükséges. Például az etikus és független munkavégzés, amelyet nem befolyásolnak és nem torzítnak a belső vagy külső szereplők. A szakértői feladatkörében nem utasítható, munkáját a függetlenség és az etikusság elvei mentén kell végeznie.¹⁵

Az egyes szakértői feladatok elvégzéséhez szükségesek az ún. digitális kompetenciák, valamint speciális, a feladat jellegéből adódóan elvárt készségek is. A kompetencia a tudás, a készségek, a képességek, a magatartásformák és a személyes jellemzők alkalmazásának vagy felhasználásának képessége, kritikus munkafeladatok, meghatározott funkciók sikeres végrehajtása, illetve adott szerepkörben vagy pozícióban való működése érdekében. A szakértői feladatok elvégzéséhez szükséges digitális kompetenciák:

- a) az információ gyűjtése, felhasználása, tárolása;
- b) digitális, internetalapú kommunikáció;
- c) a digitális tartalmak létrehozatala;
- d) problémamegoldás, gyakorlati alkalmazás;
- e) az információs és kommunikációs technológiák biztonsága.

Ezek a kompetenciák, illetve ezek alkalmazása minden vizsgálati fázisban szükséges, az alkalmazott eszközök, módszerek, technikák miatt. A speciális munkaállomások vagy azon eszközkészletek használatának készsége, amelyek a speciális vizsgálatok elvégzéséhez szükségesek, elengedhetetlen a vizsgálati célok teljesítéséhez. Minden fázisban szükséges az elvégzett műveletek és eredményeik teljes körű dokumentálása is.

Mivel a vizsgálatok magukban foglalják például a járművön belüli komponenseknek, mint például az ECU-nak, a központi egységnek (fejegység), a különböző fedélzeti egységek (*Onboard Unit*; *OBU*) adatainak vagy akár a gyártó informatikai háttérrendszerében keletkező adatoknak a vizsgálatát, ezért átfogó jármű-,

¹⁵ ERMProtect Staff [é. n.].



1. ábra. Szakértői eszközkészlet modern járművek szakértői vizsgálatához

Forrás: SCHMIDT 2022

informatikai és hálózati ismeretekre is szükség van. A vizsgálatok elvégzése során lehetőség nyílik továbbá a járműhöz csatlakoztatott fedélzeti eszközök (például kamerák) adatainak, a járműben utazók mobiltelefonjainak, valamint a jármű és a vele kapcsolatban álló egyéb kommunikációs és közlekedési infrastruktúra adatainak gyűjtésére és elemzésére is, ezért ezen eszközök használatához és működéséhez kapcsolódó ismeretek is szükségessé válnak.

A szakértői vizsgálat, a szakértői munka (meghatározott feladatok sorrendi végrehajtása) valamilyen felkérés, felhatalmazás (kirendelés) alapján kezdődik meg. Annak érdekében, hogy a szakértői vizsgálatot eredményesen, hatékonyan és a szervezeti, valamint jogszabályi követelményeknek megfelelően végezzék el, a vizsgálatot megelőző fázisban több vezetői és szakértői feladat végrehajtására is szükség van, amelyhez vezetői készségek és stratégiai gondolkodásmód is szükségessé válik.

A szakértői vizsgálat előkészítését megelőzően, a vizsgálat tervezése során szükségessé válhat a vizsgálatra felkérő személlyel, megrendelővel, kirendelővel



2. ábra. Mini Cooper műszerfalának szétszerelése
a fejegységhez való hozzáférés érdekében

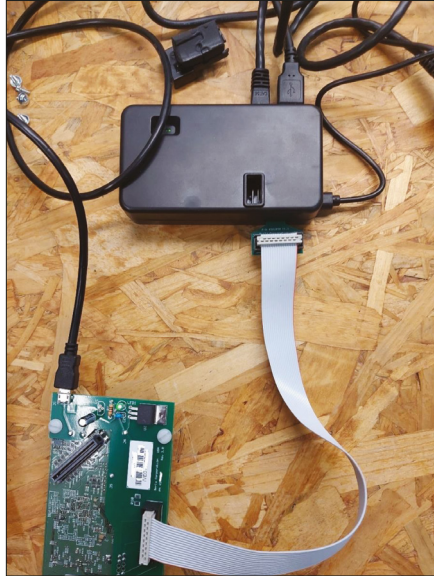
Forrás: SCHMIDT 2023

közvetlen kommunikáció is. Az általa megadott kérdések pontosítása, egyeztetése a megfelelő kommunikációs csatorna kialakításával kezdődik, majd a vizsgálati célok szükség szerinti pontosítása történik meg, valamint a vizsgálandó eseményhez kapcsolódó feladatok megtervezéséhez, meghatározásához elengedhetetlen plusz információk is beszerezhetők.

A szakértői vizsgálat tényleges megkezdése előtti fázis a vizsgálat előkészítése. Idetartozik például a szükséges vizsgálati lépések és feladatok megtervezése, az erőforrás-allokáció, a vizsgáló eszközök (például hardver-, szoftverelemek) meghatározása, amely szervezési készségeket igényel.

Az azonosítási fázisban a vizsgálat tárgyát azonosítják, vagyis a jármű azon egységeit, amelyekben digitális nyomok találhatók. Ehhez jártasság szükséges a modern járművek összetevőinek azonosításában, módosításában és kezelésében. Mivel a járművek sérülékenyek lehetnek, a szakértőnek képesnek kell lennie azonosítani olyan működéseket, amelyek eltérnek a normális működéstől. Ezt okozhatja valamilyen kártékony kód, amelynek rosszindulatú viselkedését azonosítani kell. Figyelembe véve a magas automatizáltságú járművek katonai alkalmazását, valamint az ezen a területen széles körben alkalmazott *anti-forensics* technikákat, a szakértőnek rendelkeznie kell azon készségekkel, hogy az ilyen technikák nyomait észlelni, azonosítani tudja.

Az adattároló egységekhez történő fizikai és logikai hozzáférés a modern járművek esetén összetettebb feladat. Ezeket az eszközöket védett, rejtett módon



3. ábra. Járműfejegység adatkinyeréséhez szükséges szakértői eszköz

Forrás: SCHMIDT 2023

építik be a járművekbe, ezért az előkészítési fázisban szükség van a jármű egyes részeinek fizikai szétszerelésére (például műszerfal). Ehhez a járműrészek és a fejegységek, vezérlőegységek ki- és szétszerelésének készsége is szükséges a szakértői feladatok elvégzéséhez.¹⁶

Az adatgyűjtés alatt a vizsgált esemény körülményeinek és az érintett személyek tevékenységének, hollétének és személyi körülményének tisztázását értjük, vagyis minden olyan tevékenységet, amely formális eljárásjogi keretek között a meglévő ismeretek bővítésére törekszik. Ennek kapcsán történik meg a(z):

- a) kapcsolódó adatok felkutatása;
- b) releváns adatokat tartalmazó adatforrások azonosítása;
- c) nyomok/bizonyítékok felkutatása, beszerzése, adatok kinyerése;
- d) vizsgálat megalapozásához, megtervezéséhez szükséges adatok összegyűjtése.¹⁷

¹⁶ ABForensics [é. n.].

¹⁷ PILISI 2012.

Ezen feladatok elvégzéséhez szükséges az információk gyűjtésében, feldolgozásában, kezelésében, szállításában és tárolásában való jártasság, azok integritásának megőrzése mellett. E jártasság az adatok védelme szempontjából kritikus, mert ezzel elkerülhető a vizsgálat tárgyát képező adatok szándékolatlan, váratlan megváltozása, elvesztése, fizikai károsodása vagy megsemmisülése. Az adatok gyűjtéséhez használt eszközök, (virtuális) környezetek használatának, a különböző adathordozók adatainak kinyerési készsége úgyszintén fontos.

Vizsgálati fázisban történik a kinyert adatok verifikációja, annak bizonyítására, hogy azok nem változtak a kinyerés során, valamint a vizsgálati célokhoz szükséges információk azonosítása. Ehhez szükségesek a különböző operációs rendszerek (például Windows, Linux, Automotive stb.), szakértői alkalmazások ismerete, használata. Szükséges továbbá a logikai vonatkozású *anti-forensics* technikák alkalmazásának azonosítási képessége vagy a HASH-függvények ismerete. Ebben a fázisban történik például a fájlzignatúra-összehasonlítás, vagyis az adott fájl fejlécének és kiterjesztésének összehasonlítása és jelölése, vagy az ismert fájltypusokkal való összehasonlítás (például De-NIST).

Az adatok elemzése során jellemzően valamilyen interaktív eszközzel fel kell ismerni és elemezni kell a megszerzett adatokba ágyazott adatstruktúrákat és metaadatokat. A fázis a vizsgált esemény idővonalának megalkotásához és a vizsgálati kérdések megválaszolásához szükséges releváns adatok azonosítását, a bizonyítékok meghatározását és megkeresését jelenti. Az elemzési fázisban szükséges készségek közé tartozik az elemzőeszközök használata, az események, a járműkommunikáció, az illékony adatok, a jármű-operációsrendszerek elemzése.

A vizsgálati eredmények értelmezése nagyban függ az azt megelőző fázisok eredményeitől, különös tekintettel az esetlegesen figyelmen kívül hagyott elemekre. Többféle elemző-, értelmezőeszköz segítheti a szakértő munkáját, ezek használatának készsége nélkülözhetetlen a megfelelő vizsgálati eredmények előállításához. Ezen eszközök segítenek a vizsgált eseményhez kapcsolódó adatok megértésében. Ilyen például az idővonal-eszköz, amely az események közötti kapcsolatok vizsgálatát segíti elő. Az idővonal-rekonstrukció célja a vizsgálati kérdések megválaszolása érdekében a tényállással kapcsolatos releváns események digitális nyomainak időbeli sorrendben, esetlegesen vizuális formában történő megjelenítése. Az események vizualizációjának pontos módja – táblázat, eseménynapló, digitális jelentés, térkép stb. – kötetlen, azonban tartalma minden esetben célhoz kötött. A kapcsolatelemzés megmutatja az esemény entitásai közötti összefüggéseket. A mesterséges intelligencia

fejlődésével az ún. mélytanulási technikáknak köszönhetően az egyes elemek közötti láthatatlan kapcsolatok is feltárhatók.

A részletes, átgondolt és megindokolt vizsgálati jelentések kidolgozásának és közlésének képessége szükséges ahhoz, hogy a szakértő az elvárásoknak és például a szakértői törvényben meghatározott tartalmi elemeknek megfeleljen. A dokumentációnak például tartalmaznia kell a vizsgálat módszerének rövid ismertetését, a szakmai ténymegállapításokat, a szakértő véleményét, a módszertani levélre történő utalást, illetve a módszertani levélben foglaltaktól való eltérés esetén ennek indokait stb. A szakértői vélemény tartalmára vonatkozóan további követelmények a 31/2008. (XII. 31.) IRM rendeletben találhatók, amely alapján a szakvéleménynek tartalmaznia kell:

- a) a vizsgálat tárgyára, a vizsgálati eljárásokra és eszközökre, a vizsgálat tárgyában bekövetkezett változásokra vonatkozó adatokat (lelet),
- b) a vizsgálat módszerének rövid ismertetését,
- c) a szakmai megállapítások összefoglalását (szakmai ténymegállapítás),
- d) a szakmai ténymegállapításokból levont következtetéseket, ennek keretében a feltett kérdésekre adott válaszokat (vélemény).

Amennyiben a szakértői tevékenység folyamatába beépített, a feladatok elvégzése során érvényesítendő minőségbiztosítási előírásokat alkalmaz a szervezet, akkor a soron következő fázis a validálás.

A szakértői vizsgálat validált eredménye írásos jelentés, szakvélemény, amely leírja a vizsgálatnak és a digitális adatok elemzésének az eredményeit, amely a teljes vizsgálatot vagy csak egy részét ismerteti a jogszabályi és szervezeti követelményeknek megfelelően. Ez a dokumentum képviselheti a teljes vizsgálatot vagy csak egy részét a jogi eljárás során. Egyes esetekben a jogi eljárás során a szakértő tanúként is beidézhető. A digitális bizonyítékok bemutatásának és magyarázatának képessége lehetővé teszi, hogy a szakértő egyértelmű és könnyen érthető módon ismertesse az elért eredményeket.¹⁸

¹⁸ *Workforce Framework for Cybersecurity* [é. n.]; Police Executive Research Forum 2020; MACIAG–GIORDANO 2002; TONTARSKI 2007; *Igazságügyi szakértői vizsgálatok – mik ezek?* 2021.

Összefoglalás

A különleges szakértelmet igénylő területek száma folyamatosan nő, különösen az IT, az IoT és egyéb digitális megoldásokat alkalmazó szférákban. A társadalmi viszonyok is egyre bonyolultabbá válnak, ami az igazságszolgáltatásban úgy jelent meg, hogy a peres, illetve a hatósági eljárások tárgyi és szerkezeti összetétele jelentős változáson ment át. Egyre nagyobb szerepet kapnak a szakértői vizsgálatok. A modern polgári és katonai közlekedési járművek új és egyre precízebb vezetéstámogató funkciói jelennek meg. A mesterséges intelligenciával támogatott döntéshozatal és közlekedési ágazat, a járművek komplex szenzorhálózatai új elemként jelennek meg a szakértői vizsgálatokban, amelyek célja változatlan, a releváns múlt történéseit kell hitelesen bemutatni, igazolni. Függetlenül attól, hogy a digitális nyomok milyen eszközben, milyen adattároló megoldásban találhatóak meg. Ezt a célt azonban új megoldások, módszerek, technikák alkalmazásával érhetjük el, amelyek szintén új képességeket, azok elsajátítását igénylik.

Jelen tanulmányban meghatároztam azon kulcsfontosságú készségelemeket, amelyek nélkülözhetetlenek az új típusú forenzikus vizsgálatok elvégzéséhez. Ezen készségek lehetővé teszik a vizsgálatok magas színvonalú elvégzését, a vizsgálati célok maradéktalan elérését.

A készségek elsajátítása a szakértők képzésével valósítható meg. Az alapvető számítógépes kriminalisztikai és kriminalisztikai technikák, az általános digitális kompetenciák mellett szükséges olyan készségek elsajátítása is, amelyek lehetővé teszik a vizsgálatot végző számára az egyes vizsgálati lépések speciális körülmények és eszközök esetén történő végrehajtását. Vagyis a szakértők speciális (modern járművek vizsgálatához szükséges) képességekkel való felruházását kell megvalósítani.

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 szerző külön szeretne köszönetet mondani az Alverad Technology Focus Kft. Kutatás Fejlesztés és Innováció üzletágának a kutatási munkához nyújtott támogatásáért.

Felhasznált irodalom

2016. évi XXIX. törvény az igazságügyi szakértőkről.

ABForensics [é. n.]: *Infotainment & Telematics System Data Acquisition and Analysis*. Online: <https://abforensics.com/infotainment-telematics-system-data-acquisition-and-analysis/>

BÓDI Antal (2022): *Közlekedésbiztonság fokozását megalapozó Komplex ITS Ökoszisztéma kialakításának kérdései*. PhD-disszertáció. Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola. Online: https://lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Bodi_Antal_ertekezes.pdf

CHANDEL, Raj (2020): Digital Forensics: An Introduction. *Hacking Articles*, 2020. szeptember 14. Online: www.hackingarticles.in/digital-forensics-an-introduction/

ERMProtect Staff [é. n.]: *What are the 5 Stages of a Digital Forensics Investigation*. Online: <https://ermprotect.com/blog/what-are-the-5-stages-of-a-digital-forensics-investigation/>

European Cybersecurity Skills Framework Role Profiles (2022). Online: www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

GIORDANO, Joseph – MACIAG, Chester (2002): Cyber Forensics: A Military Operations Perspective. *International Journal of Digital Evidence*, 1(2). Online: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf

GYARMATI József – SIMÓ Réka (2021) Autonóm terepjáró járművek katonai felhasználásának lehetőségei. *Haditechnika*, 55(1), 8–14. Online: <https://doi.org/10.23713/HT.55.1.02>

HEGYI Henrietta (2023): A személygépjárművek információbiztonsága az információbiztonsági szakértők szemszögéből. *Biztonságtudományi Szemle*, 5(2), 47–58. Online: <https://epa.oszk.hu/04100/04186/00020/pdf/>

Igazságügyi szakértők [é. n.]. Online: https://e-justice.europa.eu/550/HU/forensic_experts

KISS Albert [é. n.]: *Kompetenciaelemek*. Online: <https://docplayer.hu/33179006-Kompetenciaelemek-a-kompetencia-elemei-tudas-ismeret-kepesssegek-es-attitudok-amelyeket-a-kepessite-si-szint-leirasokban-az-autonomia-es.html>

NEWHOUSE, W. D. et al. (2020): National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. In PETERSEN, Rodney et al. (szerk.): *NIST Special Publication 800-18*. Online: <https://doi.org/10.6028/NIST.SP.800-181r1>

PILISI Fanni (2012): Bűnügyi adatgyűjtés, különös tekintettel a raszternyomozásra. *Büntető Törvénykönyv (új Btk.) a gyakorlatban*, 2012. december 1. Online: <https://ujbtk.hu/dr-pilisi-fanni-bunugyi-adatgyujtes-kulonos-tekintettel-a-raszternyomozasra/>

Police Executive Research Forum (2020): *Utilizing Vehicle Data in Law Enforcement Investigations*. Online: www.iacpcenter.org/wp-content/uploads/2020/09/Vehicle-Data_LECC-Article.pdf

RÉPÁS József et al. (2022): *Mit árul el rólunk az autónk? – Modern járművek IT szakértői vizsgálatának kérdései és lehetőségei*. Pécs: Szentágotthai János Szakkollégiumi Egyesület. Online: <https://doi.org/10.15170/PTE-TTK-XX.SZJMKHV>

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>

SWGDE/SWGIT (2010): *Guidelines & Recommendations for Training in Digital & Multimedia Evidence*. Online: www.crime-scene-investigator.net/swgde_swgit_training_document_v2-0.pdf

SZEGHEGYI Ágnes (2011): A tudásmenedzsment stratégiai szerepe a vállalatoknál. In NAGY Imre Zoltán (szerk.): *Vállalkozásfejlesztés a XXI. században*. Budapest: Óbudai Egyetem Keleti

- Károly Gazdasági Kar. Online: https://old2.kgk.uni-obuda.hu/sites/default/files/04_Szeghegyi%20Agnes.pdf
- The Phases of Digital Forensics* [é. n.]. Online: <https://onlinedegrees.unr.edu/blog/digital-forensics/>
- TONTARSKI, Rick (2007): *Defense Forensic Enterprise System*. Woods Hole, MA: CID Command US Army Criminal Investigation Laboratory. Online: www.nationalacademies.org/documents/embed/link/LF2255DA3DD1C41C0A42D3BEF0989ACAEC3053A6A9B/file/D3A4A5DAA-96A5C788CC027B595C0E72D5845D6AC2E57?noSaveAs=1
- TÓTH József Lukács – VÉG Róbert László (2022): Az autonóm terepjáró eszközök. *Katonai Műszaki Közlemények*, 32(2), 107–116. Online: <https://doi.org/10.32562/mkk.2022.2.8>
- Tudás - mi ez, definíció és fogalom* [é. n.]. Online: <https://hu.economy-pedia.com/11040367-knowledge>
- VÍZI Linda [é. n.]: *A Computer Forensics jogi vonzata*. Online: <https://netacademia.hu/courses/take/computer-jog/multimedia/8481853-figyelem-ez-egy-classic-tanfolyam>
- Workforce Framework for Cybersecurity (NICE Framework)* (2023). Online: <https://nccs.cisa.gov/workforce-development/nice-framework>
- YAACOU, Jean-Paul et al. (2021): Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations. Preprint. Online: <https://doi.org/10.48550/arXiv.2103.17028>