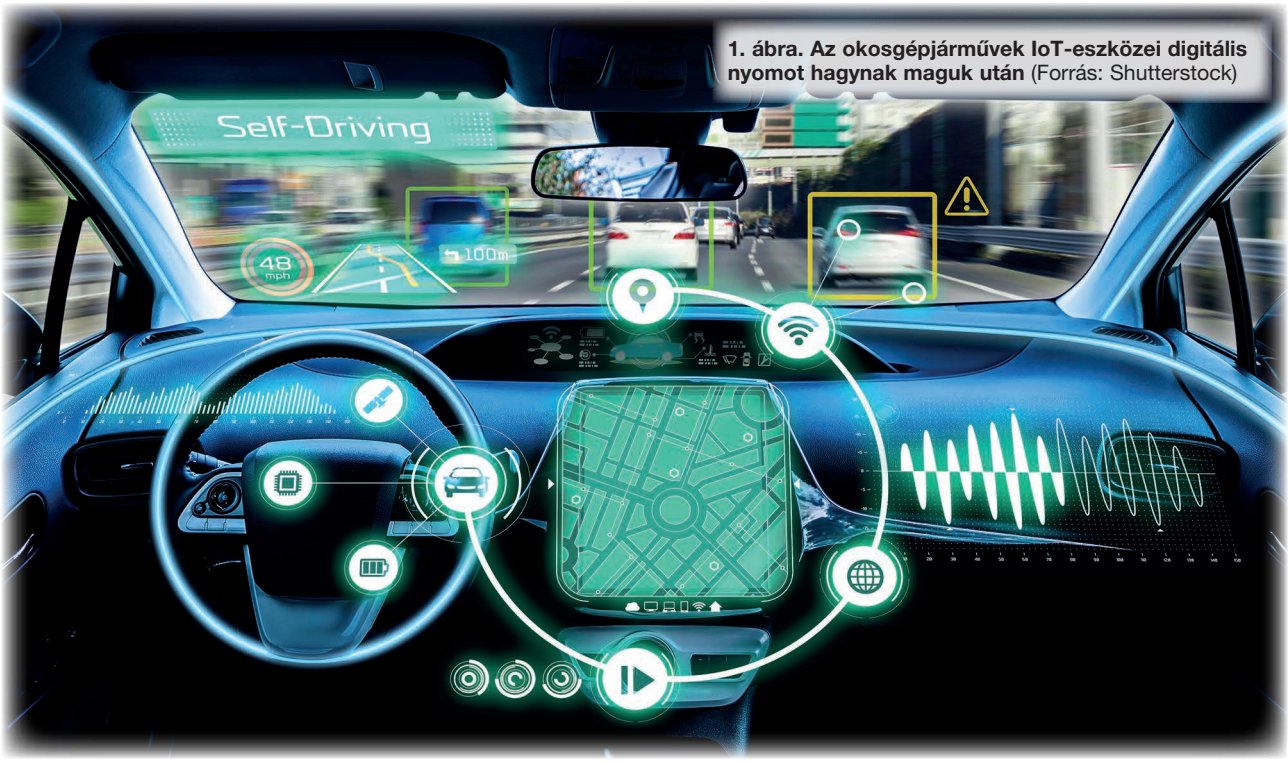


1. ábra. Az okosgépjárművek IoT-eszközei digitális nyomot hagynak maguk után (Forrás: Shutterstock)

Répás József – Pogány Viktor***

IoT forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában

Bevezetés

A katonai és polgári közlekedési eszközökkel kapcsolatos baleseteket követő, utólagos igazságügyi szakértői vizsgálatok (digital forensics – digitális igazságügyi szakértői vizsgálat) egyik célja annak megállapítása, hogy mikor, hol és milyen körülmények között történt a vizsgált esemény. Kiemelt cél például egy baleset pontos idővonalának rekonstrukciója. A vizsgálat során meg kell állapítani az esemény kiváltó okát és felelősségi körét, vagyis kinek az érintettségével és közreműködésével történt az esemény. Mindezekről hiteles bizonyítékot kell szolgáltatni, amely jogi eljárásban képes megválaszolni a vizsgálat célja szerinti kérdéseket.

Életünk számtalan feladatának elvégzéséhez használunk valamilyen digitális eszközt (például mobiltelefont, táblagépet, számítógépet). Az IoT (Internet of Things – dolgok in-

ÖSSZEFOGLALÁS: A közlekedési balesetekkel kapcsolatos, utólagos igazságügyi szakértői vizsgálatok (digital forensics vizsgálat) egyik célja annak megállapítása, hogy mikor, hol és milyen körülmények között történt az esemény. Fontos továbbá az eseménysor pontos idővonalának összeállítása, továbbá hiteles bizonyíték szolgáltatása. Jelen tanulmány célja a digitális forensics egyik területének, az IoT forensics vizsgálata annak megállapítása érdekében, hogy mely lépései vagy eljárásai alkalmazhatók a modern és egyre inkább önvezetővé váló járművek szakértői vizsgálata során.

KULCSSZAVAK: autonóm járművek, önvezető autó, szakértői vizsgálat, IoT, IoT forensics

ABSTRACT: One of the objectives of subsequent forensic expert examinations (digital forensics examination) related to transport vehicles is to establish the circumstances under which the investigated event occurred, when and where it occurred, as well as compiling its exact timeline, as well as providing credible evidence. The purpose of this study is to examine one of the areas of digital forensics, IoT forensics, to determine which steps or procedures can be used during the expert examination of modern and increasingly self-driving vehicles.

KEY WORDS: autonomous vehicles, self-driving car, digital forensics, IoT, IoT forensics

* PhD, NKE Katonai Műszaki Doktori Iskola, doktorandusz. ORCID: 0000-0002-1186-4731
** Alverad Technology Focus Kft ORCID: 0000-0002-6078-7859

2. ábra. IoT-ökoszisztémák szemléltetése (Forrás: Shutterstock)

ternete / kapcsolódó eszközök kollektív hálózata) ökoszisztémák egyre nagyobb teret nyernek például a közlekedésben, a biztonság területén, a katonai alkalmazásban és az iparban egyaránt. Az IoT-eszközök használata egyre kevésbé lesz megkerülhető feladataink elvégzéséhez. Járműveink is egyre inkább digitalizált eszközökké válnak annak köszönhetően, hogy egyre nagyobb igény mutatkozik a biztonságosabb, költséghatékony, lehetőségekben és flexibilitásban gazdag megoldásokra.

A különböző vezetéstámogató rendszerek alakalmazása miatt lépésenként szorul vissza a járművezető szerepe, akinek az automatizáltsági szintek növekedésével egyre kevesebb feladata és lehetősége lesz a közvetlen irányításra és beavatkozásra. Az egyre magasabb automatizáltsági szintű, egyre inkább önvezetővé váló járművek kamerákkal és szenzorokkal térképezik fel környezetüket. Az érzékelők adatainak, valamint a jármű által generált adatok átviteléhez és feldolgozásához (a járművön belül és azon kívül egyaránt) összetett kommunikációs hálózat és nagy számítási teljesítmény szükséges. Az új eszközök és kapcsolatok, a szoftverorientált járműgyártás, a felhőalapú megoldások a közlekedési ökoszisztémában történő elterjedése új támadási irányok megjelenését is eredményezik. A jelenlegi szabályzók értelmében a gyártók és szoftverfejlesztők felelőssége a járművek közlekedés- és kiberbiztonsági kockázatainak kezelése, azonban előre nem látható események, szoftver-sérülékenységekből eredő balesetek a jövőben is előfordulhatnak. Ezeket utólagos szakértői vizsgálatok során vizsgálni kell. A vizsgálatok elvégzéséhez megfelelő eszközök, módszerek, képességek és tudáselemek szükségesek mind a polgári és nemzetbiztonsági szakértői intézetek, mind a katonai alkalmazás területén. [30]

Járműveink – más digitális eszközeink használatához hasonlóan – digitális nyomot hagynak maguk után. Ezek a nyomok – amelyek az egyre komplexebbé váló, magas automatizáltságú járművek esetén már szinte kivétel nélkül digitális formában jelennek meg, bináris formában tárolódnak és továbbítódnak – [22][26][29], bizonyítékként felhasználhatók egy igazságügyi szakértői vizsgálat során. Megállapíthatóvá válhat például, hogy a járművezető mit tett, mikor és hol volt, kivel találkozott. Napjaink járművei is jóval több adatot tárolnak rólunk, mint amennyit egy átlagos felhasználó gondolna. Az ilyen adatok köre a jövőben tovább szélesedik, így hasznos bemenetet jelent majd a szakértői vizsgálat során az adatok elemzéséhez, a nyomok értelmezéséhez.

A digitális információk járművekből történő begyűjtése, új kihívás elé állítja a (katonai) nyomozati és igazságszolgáltatási tevékenységeket támogató, digitális forenzikus vizsgálatot végző szakértőket. A közlekedési ökoszisztémában alkalmazott összetett informatikai és infokommunikációs rendszerek miatt, valamint a járművek által gyűjtött és feldolgozott adatmennyiség közel exponenciális növekedésének eredményeként, a már meglévő szakértői vizsgálati eljárások nem, vagy csak korlátozott módon lesznek alkalmazhatók.

A meglévő digitális forenzikus eszközök és technikák részben vagy egészben felfedhetik a járművekben megtalálható adatokat. Szükséges azonban annak előzetes vizsgálata, hogy mely eszközök és technikák, milyen feladatok elvégzésére, mely adatokhoz való hozzáférés biztosítására alkalmasak, továbbá az egyes eljárásoknak milyen korlátai vannak. Mint minden módszernek, a digitális szakértői vizsgálatoknak is megvannak a maga korlátai „a releváns múlt megismerése sokszor szinte leküzdhetetlen akadályokba ütközhet, és mindig fennáll a tévedés veszélye is” [12], ennek megértése fontos a módszerek alkalmazásához és a vizsgálatok elvégzéséhez.

Nem létezik egyetlen olyan technika, amely a digital forensics egyetemes technikájának tekinthető. Technikák ezrei állnak rendelkezésre, amelyek a szakértői vizsgálat során használhatók, így a vizsgálatoknak számos egymástól eltérő, mégis hasznos modellje létezik. Jelen tanulmány célja a digitális igazságügyi szakértői egyik területének, az IoT forensics-nek a vizsgálata, annak megállapítására, hogy annak mely lépései, vagy eljárásai alkalmazhatók a modern és egyre inkább önvezetővé váló járművek szakértői vizsgálata során. [7][22][26][29]

Az IoT forenzikus vizsgálat

Az IoT-eszközök csoportjába minden olyan eszköz, érzékelő, objektum beletartozik, amelyek emberi beavatkozás nélkül képesek kommunikálni egymással, céljuk az információ begyűjtése és szolgáltatása. Internetcsatlakozáson keresztül (vagy valamilyen szeparált hálózatban) képesek különböző sztenderdizált kommunikációval megosztani az adatokat, autonóm módon interakciókat folytatnak egymással, a felhasználóval, a központi rendszerrel, felhővel stb. Az IoT megjelenése az emberek, a szolgáltatások, az érzékelők és a tárgyak átfogó kapcsolatához vezetett. [23] A mára már több milliárd eszközt magában foglaló IoT-ökoszisztéma bővülése, a járművekben történő megjelenése és elterjedése hatalmas mennyiségű adatot generál, amely új kihívást jelent a forensics szakértők számára. Az International Data Corporation (IDC) 2019-es jelentésében úgy becsülte, hogy a csatlakoztatott IoT-eszközök 2025-ig megközelítőleg 79 zettabájtnyi (10^{21} bájt) adatot generálnak. Ezek egy része a magas automatizáltságú járművek adatai lesznek, amelyek potenciális bizonyítékként szolgálhatnak a szakértői vizsgálatok során. [15][16]

Az IoT-eszközök katonai területen is megjelennek, nemzetközi vonatkozásban az alábbi felhasználási területeken töltenek be nagy szerepet:

- a katonai teljesítmény nyomon követése;
- a katonák egészségügyi felügyelete;
- a pilóta nélküli rendszerek elterjedése;
- a populáció nyomon követése;
- a logisztikai feladatok hatékonyabb elvégzése;
- a műveleti döntések meghozatalához szükséges nagy mennyiségű adat biztosítása;
- a katonai objektumok és kritikus infrastruktúrák védelmét elősegítő megoldások bevezetése. [34]

Az IoT-eszközök új biztonsági és forenzikus vizsgálati problémákat is felvetnek, mind polgári, mind katonai szem-

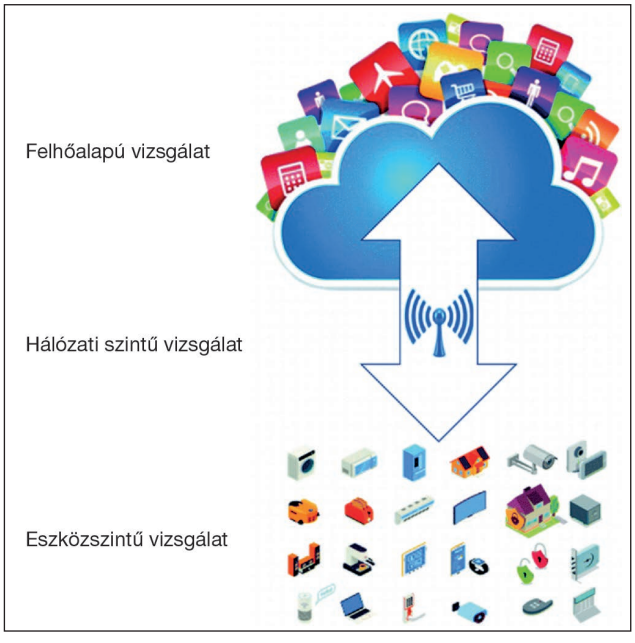
pontból. Az egymással kommunikáló nagyszámú eszköz, sok esetben nem megfelelő biztonsági intézkedések mellett működik. Az érzékeny adatok egyre nagyobb részét teszik ki az általuk generált hálózati adatforgalomnak, ezáltal egyre népszerűbb célpontjai a különféle kibertámadásoknak, ami adott esetben nemzetbiztonsági kockázatot is jelenthet. Az IoT-eszközök heterogén természete és a szabványok hiánya megnehezíti a klasszikus digitális forensics eljárások átvételét.

Az intelligens járművek térnyerésének alapvető elemei az IoT- és a különböző kiberfizikai eszközök, szenzorok, környezetek, amelyek utólagos igazságügyi szakértői vizsgálata nélkülözhetetlen eleme az események rekonstruálásának. Az IoT forensics célja az IoT-vel kapcsolatos események, az internetes csatlakozással rendelkező eszközök, szenzorok által előállított, továbbított és tárolt adatok forrásainak megállapítása, az adatok azonosítása, begyűjtése, vizsgálata. Az IoT forensics terület magában foglalja a különböző IoT-eszközökből származó digitális bizonyítékok széles skálájának megszerzését, megőrzését és elemzését, a kapcsolódó alkalmazásokat, az internetet és a felhő alapú technológiát, magukat az eszközöket és más kapcsolódó rendszereket, amelyek az IoT-ökoszisztéma (polgári vagy katonai) részeként működhetnek. [8][9][17][31]

A szakértői vizsgálatokban a „vizsgálat” szó „nem egy jogilag szabályozott eljárási formát, hanem az ismeretszerzés egy módszerét jelenti”. [10] Ennek során a fő cél, az egyes eseményekhez, bűncselekményhez vagy balesethez kapcsolódó kulcsfontosságú bizonyítékok azonosítása, elemzése, utólagos vizsgálata. Meg kell állapítani a felelősségi kérdéseket, hogy mi, mikor, hol, hogyan történt és ki volt érintett, valamint a megtörtént események igazolása is szükséges. IoT-eszközök (például szenzorok, szenzorhálózatok), rendszerek (például digitális eszközökkel felszerelt vagy önvezető járművek) vizsgálata esetén is érvényesek ezen célok és elvárások. Az IoT területén három vizsgálati szintet (*3. ábra*) különböztetünk meg:

– eszközszintű vizsgálat,
– hálózati szintű vizsgálat,
– felhőalapú szakértői vizsgálat. [16]

3. ábra. Az IoT szakértői vizsgálat három szintje
(A szerző szerkesztése [35] alapján)



Az ENISA (European Network and Information Security Agency – Európai Uniós Hálózat- és Információbiztonsági Ügynökség) az IoT-ben szereplő (things) dolgokat olyan fizikai vagy virtuális tárgyként, eszközként definiálja, amelyek kommunikációs hálózatokba integrálhatók, és képességeiktől, kapacitásuktól függően, különböző funkciókat biztosítanak. Ilyen funkció lehet a teljesség igénye nélkül az adatok érzékelése és rögzítése, továbbítása, tárolása és feldolgozása, vagy valamilyen beavatkozási művelet végrehajtása, illetve alkalmazások futtatása vagy a gépi tanulás.

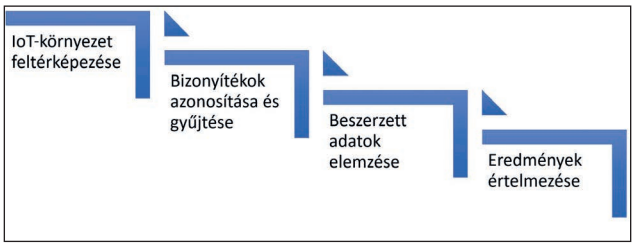
Eszközszintű vizsgálatok esetén, elsődleges bizonyíték forrásként maga az IoT-eszköz szerepel. Az IoT-eszközök szakértői vizsgálatba számos eszköz bevonható, például érzékelők, egészségügyi implantátumok, nyomkövető eszközök, intelligens mérők, okos háztartási készülékek, okoskamerák, hálózatba kapcsolt járművek és drónok. Mivel az eszközök hardverükben és funkcióikban különböznek egymástól, a bizonyítékok azonosítása és megszerzése gyakran nagy kihívást jelent, és nem mindig kivitelezhető. [18]

Hálózati szintű vizsgálatok esetén az IoT-eszközöket egymással összekötő különféle kommunikációs hálózatok eseményeinek vizsgálata történik. Ez a hálózati forgalom, az információk és események begyűjtése, rögzítése és elemzése annak érdekében, hogy egy hálózat elleni támadás forrása megállapítható legyen, és sor kerülhessen egy behatolás észlelésére, illetve vizsgálatára. [1][2][5][24]

A felhőalapú megoldások elterjedésével digitális átalakulás történik. Mivel az IoT-eszközök korlátozott adattárolási és feldolgozási képességekkel rendelkeznek, az általuk generált adatokat vagy azok egy részét továbbítják egy felhőszolgáltatáshoz további feldolgozás és tárolás céljából, így a felhő a szakértői vizsgálati folyamat egyik fő részévé válik. A szoftverektől kezdve a különböző platformokon át, az infrastruktúráig egyre több mindent veszünk igénybe szolgáltatásként, nem kivétel ez alól a járműipar sem. Napjainkban a személyes és vállalati adatok több, mint felét valamilyen felhőalapú megoldásban tárolják. Ezen rendszerek, megoldások esetén is szükségessé válhat az események utólagos elemzése, vizsgálata. Definíció szerint a Cloud forensics, vagyis felhő alapú rendszerek szakértői vizsgálata a digital forensics alkalmazása felhőkörnyezetekben, ahol virtuális szerverek és hálózatok, „vékony” és „vastag” kliensek[1], távoli elérések stb. vizsgálata történik a szükséges bizonyítékokhoz történő hozzáférés érdekében. Mind a felhőszolgáltató, mind a szolgáltatást igénybe vevő, mind a közvetítő oldaláról szükséges lehet valamilyen információ a vizsgálatok végrehajtásához, azonban a határvonalak összemosódhatnak azzal kapcsolatban, hogy a feltárt bizonyíték kihez tartozik. A szolgáltatások típusai határozzák meg, hogy milyen szabályok érvényesek, amelyek szervezeti, technikai – az adatok a helyszínen kívül több helyen, vagy egy harmadik fél tulajdonában lévő szerveren is tárolásra kerülhetnek – és jogi problémákat is felvetnek, továbbá a többes joghatóság kérdésének kezelését is jelentheti. Jelen tanulmány nem tér ki részletesen a hálózat vizsgálatára és cloud forensics (felhő alapú rendszerek vizsgálatai) eljárásokra, ezek további kutatási feladatok részét képezik [4][13][16][20][21][25][32].

IoT FORENSICS FOLYAMATA

Az IoT-eszközök vizsgálata során is elsődleges a digitális bizonyítékok, elektronikus adatok időben történő kinyerése és megőrzése, amely nagy kihívást jelent a szakértők számára, mert ezeket az eszközöket passzív és autonóm mű-



4. ábra. Az IoT forensics folyamat fázisai (A szerző szerkesztése)

ködésre tervezték. Amikor egy IoT-eszközt releváns adatforrásként azonosítanak a vizsgálati folyamat során, nincs dokumentált módszer vagy megbízható eljárás az eszközön megtalálható bizonyítékok megfelelő összegyűjtésére. Ezek hiányában a digitális forensics módszereket az IoT speciális online karakterisztikájához, lehetőségeihez és igényeihez illesztik. A szakértői vizsgálat IoT környezetben is csak valamilyen törvényes felhatalmazás alapján kezdődhet meg. *(4. ábra)*

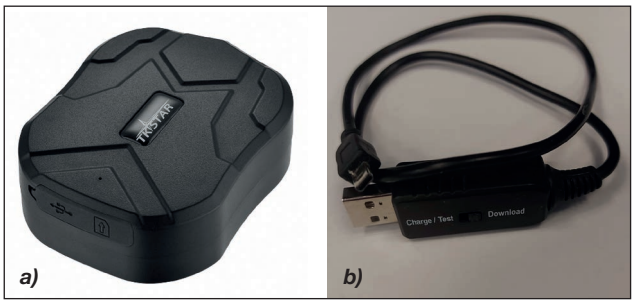
Az IoT-környezet feltérképezése

Első lépés a vizsgálandó IoT-környezet feltérképezése, amely a vizsgálat céljának megfelelő bizonyítékokat tartalmazza (bizonyítékok azonosítása). Ebben a fázisban megismerhetők például a hálózatban található eszközök, a felhasznált hardverek és szoftverek típusai, az operációs rendszer, valamint a digitális bizonyítékok típusa és mennyisége, azok tárolási módja (helyi vagy távoli), a felhasználók biztonsági szintje, és az esetlegesen alkalmazott anti-forensics megoldások.

Bizonyítékok azonosítása és gyűjtése

A vizsgálat sikeres elvégzéséhez kapcsolódóan az adatgyűjtési lépéseknek annyi információ azonosítását és összegyűjtését kell biztosítani, amennyi csak lehetséges az adott IoT-környezetben. Továbbá biztosítani kell a megszerzett adatok integritását, és stabil forrást kell biztosítani az adatok elemzéséhez. Adatgyűjtés alatt a vizsgált esemény körülményeinek, az érintett személyek tevékenységének, hollétének és személyi körülményeinek tisztázását értjük. Idetartozik minden olyan tevékenység, amely formális eljárásjogi keretek között, a meglévő ismeretek bővítésére törekszik. [11]

A lehetséges bizonyítékok összegyűjtése magában foglalhatja az IoT-ökoszisztéma különböző rétegeinek vizsgálatát. Az interfész rétegben nyílik lehetőség a különböző API-k (application programming interface – alkalmazásprogramozási felület) vizsgálatára, a tartalmak visszakeresésére, a hozzáférésekhez kapcsolódó információk, nyomok keresésére (digitális ujjlenyomatok, vagy egyéb felhasználói hozzáférések). Azonosíthatóvá válhatnak potenciális gyanúsítottak, egyéb érintettek a biometrikus bizonyítékok, vagy személyes login információk segítségével. A szolgáltatási rétegben találhatók az azonosított szolgáltatásokra, forgalomra és a felhasználókra vonatkozó információk, például SLA (service level aggreement – szolgáltatásiszint-megállapodás). A hálózati rétegben az eszközök, adatforrások internet-, illetve felhő használatára vonatkozó információk találhatók. Forrás és cél IP-címek, adatfolyam, közösségi médiahasználat, kártékony alkalmazások részletei állapíthatóak meg az eseménynapló állományok gyűjtése és elemzése alapján. Az érzékelő rétegben található az IoT-rendszer fentebb tárgyalt



5. ábra. GPS nyomkövető készülék *a)* és a vizsgálatához szükséges adatletöltő kábel *b)* (Forrás: [14], a jobb oldali kép a szerző felvétele)

dologi, vagyis eszköz része. Idetartoznak a szenzorok, az okoselemek és a csatlakoztatott médiaeszközök. Az IoT-hardver cache-ben vagy a memóriában található adatainak elemzése után meghatározhatják például az eszköz használati helyét is. [28]

A digitális adatok kinyerésének alapvető technikája a vizsgálandó adatokról történő másolat készítése. Az IoT-eszközök esetén ez a módszer az adattároló képességgel rendelkező eszközök adattartalmának megszerzését jelenti. Az egyik legegyszerűbb módja ennek a logikai adatgyűjtés, ami az eszközön található minden digitális nyom közvetlen kinyerését jelenti magáról az eszközről; valamilyen szabványos csatornán (például USB-csatlakozás), speciális kábel segítségével. Az *5. ábrán* látható GPS-nyomkövető eszköz vizsgálatához szükséges USB csatlakozókábel segítségével nyílik lehetőség.

Szelektív adatgyűjtés esetén a támogatott digitális adatoknak csak egy részét nyerik ki az eszközről, célzott módon, a vizsgálat célja szerinti adatok letöltése történik meg.

Az IoT-eszközök széles köre miatt eltérő fájlrendszerszerkezetek és tartalmak is előfordulhatnak, a vizsgálat elvégzéséhez szükség lehet az eszköz fájlrendszerének kinyerésére is. Ez lehetővé teszi a felhasználó számára látható összes adat megszerzését.

Fizikai adatgyűjtés esetén az IoT-eszköz fizikai tárolójáról készül teljes másolat. Ez a módszer több komponensből álló, komplex eszközök esetén fizikai beavatkozást jelent, például a memóriacsip eltávolítását (chip-off) vagy a memóriacsipek közvetlen elérésére szolgáló JTAG[2]-pontokon keresztül, vagy UART[3] segítségével. A JTAG módszer a legteljesebb, lehetővé teszi a korábban törölt adatok helyreállítását is.

Az IoT-eszközök mobil kommunikációjának megvalósítását egy szolgáltatói SIM-kártya segítségével valósítják meg, így a kártya adatai is hozzájárulhatnak a vizsgálat sikeréhez.

Távoli adatgyűjtés az egyik legelterjedtebb megoldás az IoT-eszközök és -rendszerek esetén, figyelembe véve, hogy az eszközök földrajzilag jól elkülönített módon helyezkedhetnek el. A hálózaton keresztül történő hozzáférés esetén, az eszköz összes adatának elérése nem minden esetben valósítható meg, hasonlóképpen az írásblokkoláshoz. [7]

Az IoT-környezet és az adatok feltérképezése után az általános digitális forensics módszertan szerinti lépések következnek, az IoT sajátosságait és elemeit figyelemmel kísérve. [31]

Beszerzett adatok elemzése

Az adatok kinyerése után, azok elemzése a szakértői vizsgálat következő lépése. A számítógépes környezetek forensics vizsgálata esetén ez nagyrészt valamilyen inter-

aktív eszközzel történik, amely felismeri és elemzi az adatok struktúráját, és a metaadatokat. IoT-ökoszisztémára vonatkozóan ilyen megoldások nem, vagy csak korlátozott módon és bizonyos feltételekkel alkalmazhatók. A kinyert adatok azonosításának és kibontásának célja a vizsgált esemény idővonalának megalkotása (releváns adatok azonosítása és megkeresése), amely hozzájárul a vizsgálat során felmerülő kérdések megválaszolásához. Releváns digitális nyomok többféle módon kinyerhetők az adathalmazból, például kulcsszavas kereséssel, dokumentum lekéréssel, metaadat-attribútum egyeztetéssel, hash-függvény[4] alapú kereséssel, vagy szabványos formátumú üzenetek keresésével.

Eredmények értelmezése

Számos fontos szempontot kell figyelembe venni az eredmények értékeléséhez, értelmezéséhez. Ilyen lehet a releváns adatok jelentése az adott vizsgálat szkópjára vonatkozóan, az elfogultságot csökkentő intézkedések, a vizsgálat lefolytatását akadályozó tényezők, a rendszerórák aszinkron működése stb. A vizsgált eseményhez tartozó adatok megértésében elemző eszközök is segíthetnek. Ilyen elemző eszköz például az idővonal eszköz, amely az események közötti kapcsolatok vizsgálatát segíti úgy, hogy időbeli sorrendbe helyezi az egyes eseményeket. A kapcsolatelemzés megmutathatja az esemény entitásai közötti összefüggéseket, például, hogy melyik eszköz milyen irányba, vagy ki kivel kommunikált a vizsgált esetben. A mesterséges intelligencia lehetőségei is egyre szélesebb körben alkalmazhatók lesznek annak érdekében, hogy az esetelemek közötti láthatatlan kapcsolatokat feltárják vagy az adatok között releváns elemeket ismerjenek fel.

A szakértői vizsgálat eredménye egy írásos jelentés, amely leírja a vizsgálat és a digitális adatok elemzésének eredményeit, összeállítja a vizsgált eseményről szóló narratívát, amely a jogi eljárás során képviselheti a teljes vizsgálatot vagy annak egy részét.

IoT szakértői vizsgálat kihívásai a modern járművek adatelemzésekor

Az IoT a szobai hőmérséklet szabályozásától kezdve, az önvezető járművekig teljesen behálózza a mindennapi életünket. A közlekedési balesetekkel kapcsolatos eredményes vizsgálat elvégzéséhez szükséges, hogy ebben a kiterjedt hálózatban a bizonyítékok felkutatása és begyűjtése időben megtörténjen. Mivel az IoT-eszközöket passzív és autonóm működésre tervezték, nem áll rendelkezésre dokumentált módszer vagy megbízható eszköz az ilyen eszközön megtalálható bizonyítékok közvetlen összegyűjtésére.

Nem minden IoT-eszköz tárol olyan metaadatokat, mint például az időinformáció. Ennek hiányában a különböző IoT-eszközökről gyűjtött bizonyítékok időbeli összefüggéseinek megállapítása szinte lehetetlen. A vizsgálatok során a dinamikusan változó környezet miatt előfordulhat, hogy az ideiglenes naplóállományok nem elérhetők, a hálózat bizonyos része nem vizsgálható. Korlátozott módszerek állnak rendelkezésre egy adott IoT-eszköz, vagy környezet lemezképének (image) létrehozására. A valós idejű és autonóm interakciók az eszközök között megnehezítik, sőt akár lehetetlenné is teszik az eszköz vagy rendszer komp-

6. ábra. Az utólagos igazságügyi szakértői vizsgálatok a gépjárművek IoT-eszközeinek/-szenzorainak adatai alapján rekonstruálják, hogy mikor, hol és milyen körülmények között történt a közlekedési esemény (Forrás: Shutterstock)

romittálódásának, hatókörének, és a cselekmény helyszínhatárainak azonosítását. Ilyen esetekben a lehető legtöbb bizonyíték összegyűjtésére kell törekedni. [6][27]

Az eszközökön belüli megfelelő hitelesítés nélkül nem minden esetben azonosíthatók a tevékenységek és azok felelőse. Az IoT-környezetekben nem minden esetben létezik biztonságos naplózás és monitorozó rendszer sem. Az IoT-környezetek gyors fejlődési üteme és természete számos biztonsági és forenzikus vizsgálati kihívást jelent. [23]

Ahogy a járműveink egyre inkább összekapcsolódnak és autonómmá válnak, a járművek internete (IoV – Internet of Vehicles) megjelenésével megnő a szakértői vizsgálatok szerepe, fontossága és szükségessége. Figyelembe kell venni azt a tényt, hogy a járművezetők nem kizárólagosan lesznek felelősek a balesetekért, ugyanis a balesetek történhetnek szoftver- és hardverhibák, kibertámadások miatt is. Így olyan eset is felmerülhet, hogy amennyiben a baleset oka egy szoftver- vagy hardverkomponens hibája, akkor az eladó/gyártó manipulálhatja az eseményadatokat, hogy elkerülje, vagy csökkentse a következményeket, emiatt az adatok hamisítás elleni védelme is szükséges. [3]

Az IoT-eszközök (ideértve a járművekben található eszközöket is) és azok kapcsolatainak azonosítása, a hálózat komplexitása és fizikai elosztottsága miatt nem minden esetben egyszerű feladat. Az azonosítás teljeskörűsége, minden eszköz azonosítása – mérettől vagy funkciótól függetlenül – fontos szempont, mivel a hálózat részét képezik, és tartalmazhatnak olyan információt vagy sérülékenységet, amely a vizsgált esemény szempontjából releváns lehet.

Összegzés

Az intelligens járművek térnyerésének alapvető elemei az IoT-, és a különböző kiberfizikai eszközök, szenzorok, környezetek, amelyek utólagos igazságügyi szakértői vizsgálata nélkülözhetetlen eleme a megtörtént események rekonstruálásának. Az IoT forensics módszertan célját, lépéseit és kihívásait áttekintve megállapítható, hogy mivel a járművek komplex IoT-rendszernek is tekinthetők, a modern és egyre inkább önvezetővé váló járművek esetén az IoT-eszközök jelen tanulmányban tárgyalt szakértői vizsgálati lépései alkalmazhatók, különös tekintettel az eszközök és adatok feltérképezésére. Az alkalmazott eszközök tekintetében azonban a járművek esetén komplexebb eszközök és hozzáférési módok szükségesek egy vizsgálat elvégzéséhez. Az IoT-eszközökhöz hasonlóan a járművek is számos olyan nyomot is generálnak, amelyek nem járulnak hozzá a vizsgálat hatékony elvégzéséhez, ezért kiemelt feladat a valóban hasznos információk kiszűrése az irreleváns információk közül. A digitális adatok megszerzése, vagy az azokhoz történő hozzáférés biztosítása az IoT-környezetekben sem mindig egyértelmű feladat, az adatok integritásának biztosítása azonban elsődleges, figyelembe véve a gyártók esetleges érdekellentétét (például közlekedési baleset vagy terrortámadás esetén).

Az IoT-hez kapcsolódó szakértői vizsgálati szintek a modern járművekben is megjelennek, járművek vizsgálata esetén is különbséget kell tenni az eszköz szintű, hálózati szintű vizsgálat, és a felhőalapú megoldások vizsgálatában. Ezen szintek adatforrásainak és adatainak elemzése ezen járművek esetén is elengedhetetlen.

Köszönetnyilvánítás

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

A tanulmány az Innovációs és Technológiai Minisztérium a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból, a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal útján a Kooperatív Doktori Program Doktori Hallgatói Ösztöndíjjal finanszírozott szakmai támogatásával készült.

Innovációs és Technológiai Minisztérium

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

Hivatkozott irodalom

[1] Abeis Ab, Iot forensics, https://www.slideshare.net/AbeisAb/iot-forensics-11792666 (Letöltve: 2022.12.12.);
[2] Jinadasa, Anuka. IOT Forensic Challenges, 2021. https://www.slideshare.net/AnukaJinadasa/iot-forensics-249699308 (Letöltve: 2022.12.12.);
[3] Abhay, P. A., Jishnu, N. V., Meenakshi, K. T., Yaswanth, P. S., Philip A. O. Auto Block IoT: A Forensics Framework for Connected Vehicles https://www.researchgate.net/publication/352186853_Auto_Block_IoT_A_Forensics_Framework_for_Connected_Vehicles, DOI 10.1088/1742-6596/1911/1/012002 (Letöltve: 2022.12.12.);
[4] Shiklo, Boris. Automotive IoT: Smarter Vehicles, Optimized Car Manufacturing https://www.scnsoft.com/blog/iot-in-automotive-industry (Letöltve: 2022.12.12.);
[5] Liu, Changwei. Anoop Singhal and Duminda Wijesekera, A logic-based network forensics model for evidence analysis https://csrc.nist.gov/CSRC/media/Projects/Measuring-Security-Risk-in-Enterprise-Networks/documents/logic_based_network_forensices_model-for_evidence_analysis.pdf (Letöltve: 2022.12.12.);
[6] Al-Dhaqm, A., Adeyemi, I. R., Kebande, V.R., Abd Razak, S., Grispos, G., Choo, K. R., Al-rimy, B. A. S., Rahman, A., Alsewari, A. Digital Forensics Subdomains: The State of the Art and Future Directions, 2021. https://www.researchgate.net/figure/IoT-Forensics-Issues_fig1_355762006 (Letöltve: 2022.12.12.);
[7] Lyle, J. R., Guttman, B., Butler, J. M., Sauerwein, K., Reed, Ch., Lloyd, C. E. Digital Investigation Techniques: A NIST Scientific Foundation Review https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354-draft.pdf (Letöltve: 2022.12.12.);
[8] Karthika, D. 2021. IoT Sensors: Security in Network Forensics https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119769057.ch8 https://doi.org/10.1002/9781119769057.ch8 (Letöltve: 2022.12.12.);
[9] Dolgok internete http://industry4.hu/hu/fogalomtar/dolgok-internete-iot (Letöltve: 2022.12.12.);
[10] Bócz Endre, Lakatos János. A kriminalisztika egyes aktuális elméleti kérdései, Kriminalisztikai jegyzetek és tanulmányok, RTF Kriminalisztikai Tanszék, 2008. https://docplayer.hu/4963263-Dr-bocz-endre-dr-lakatos-janos.html (Letöltve: 2022.12.12.);
[11] Pilisi Fanni. Bűnügyi adatgyűjtés, különös tekintettel a raszternyomozásra, 2012. https://ujbtk.hu/

dr-pilisi-fanni-bunugyi-adatgyujtes-kulonos-tekintettel-a-raszternyomozasra/ (Letöltve: 2022.12.11.);
[12] Finszter, G. A kriminalisztika ígérete, Magyar Tudomány 2020/5. https://mersz.hu/hivatkozas/matud_f41567/#matud_f41567 (Letöltve: 2022.10.15.);
[13] Forensics technologies https://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies (Letöltve: 2022.12.24.);
[14] Forrás: https://nyomkovetes.net/termek/tkstar-tk905b-10000mah-magneses-gps-nyomkoveto-gps-nyomkovetes?gclid=EAIaIQobChMI5e6A0JGu_AIVF-13Ch1vAw4nEAQYAyABEgIUxfD_BwE (Letöltve: 2023.1.4.);
[15] Kebande, V., Mudau, P., Adeyemi, I., Venter, H., Choo, K. R. Holistic digital forensic readiness framework for IoT-enabled organizations https://www.researchgate.net/publication/342880218_Holistic_Digital_Forensic_Readiness_Framework_for_IoT-Enabled_Organizations DOI: 10.1016/j.fsir.2020.100117 (Letöltve: 2022.11.10.);
[16] Atlam, H. F., Hemdan, E. E., Alenezi, A., Alassafic, M. O., Wills, G. B. Internet of Things Forensics: A Review 2020 February, DOI: 10.1016/j.iot.2020.100220;
[17] IoT biztonság https://www.ldsz.hu/iot-a-dolgok-internete-es-a-biztonsagtechnika-1-resz-68 (Letöltve: 2022.12.12.);
[18] IoT forensics https://en.wikipedia.org/wiki/IoT_Forensics (Letöltve: 2022.11.24.);
[19] McGhiey, K. Internet of Things (IoT) Forensics előadás, 2020. https://www.youtube.com/watch?v=rpgSNilu_X0, (Letöltve: 2022.12.12.);
[20] Ruan, K., Carthy, J., Kechadi, T., Baggili, I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results, Digital Investigation, https://www.sciencedirect.com/science/article/abs/pii/S1742287613000121 (Letöltve: 2022.11.12.);
[21] Ruan, K., Carthy, J., Kechadi, T., Crosbie, M. Cloud forensics: An overview https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview (Letöltve: 2022.11.11.);
[22] Máté I. Zs. Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe http://real.mtak.hu/116025/1/MateIstvanZsoltBelugyiSzemle2018.evi7-8.szam36-54.pdf DOI: 10.38146/BSZ.2018.7-8.3 (Letöltve: 2022.12.12.);
[23] Conti, M., Dehghantanha, A., Franke, K., Watson, S. "Internet of Things Security and Forensics: Challenges and Opportunities", (Elsevier) Future Generation Computer Systems Journal, DOI: https://doi.org/10.1016/j.future.2017.07.060, 2018;
[24] Network forensics https://resources.infosecinstitute.com/topic/network-forensics-overview/ (Letöltve: 2022.12.10.);
[25] Joshi, R. C., Pilli, E. S. Cloud Forensics, Fundamentals of Network Forensics, ISBN: 978-1-4471-7299-4;
[26] Répás J., Berek L., Schmidt M. Autonomous Vehicles Forensics -The next step of the Digital Vehicles Forensics, 1ST IEEE INTERNATIONAL CONFERENCE ON COGNITIVE MOBILITY, 2022.10.12-13.;
[27] Security In IoT Forensics https://arcnovo.tech/our-insight/security-in-iot-forensics (Letöltve: 2022.12.11.);
[28] Sathwara, S., Dutta, N., Pricop, E. IoT Forensic - A digital investigation framework for IoT systems, ECAI 2018 - International Conference – 10th Edition Electronics, Computers and Artificial Intelligence 28 June - 30 June 2018, Iasi, Romania, https://arxiv.org/ftp/arxiv/papers/1909/1909.02815.pdf (Letöltve: 2022.12.12.);
[29] SWGDE/SWGIT Digital & Multimedia Evidence Glossary Version: 1.0 (2005) https://www.swgde.org/documents/Archived%20Documents/SWGDE-SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary%20v1-0 (Letöltve: 2022.5.11.);
[30] The car is going to become an IoT device on wheels https://www.bosch-mobility-solutions.com/en/mobility-topics/iot-device-on-wheels/ (Letöltve: 2022.11.13.);
[31] Flaglien, A. O. The Digital Forensics Process https://www.researchgate.net/publication/318198370_The_Digital_Forensics_Process, DOI: 10.1002/9781119262442.ch2 (Letöltve: 2022.12.12.);
[32] Török Péter. Titkos üzenet száll a széllel! (IoT-ben használt vezeték nélküli adatátviteli technológiák összehasonlítása), Hadmérnök, XIV. évfolyam 3. szám 2019.;
[33] Gehlot, A., Singh, R., Singh, J., Sharma, N. R. 2022. Digital forensics and the internet od things ISBN: 978-1-119-76878-4;
[34] Kollár Csaba. Az IoT katonai felhasználási lehetőségei és a fejlesztési irányai, Hadmérnök, XII. Évfolyam 4. szám 2017.;
[35] Forrás: https://www.researchgate.net/figure/Investigation-process-of-IoT-forensics_fig4_337259162, (Letöltve: 2023.1.10.);
[36] Forrás: https://www.shutterstock.com/image-photo/digital-transformationiot-internet-things-transformation-modern-2054921279 (Letöltve: 2023.2.16.).

Jegyzetek

1 A kliens olyan alkalmazás vagy rendszer, amely egy távoli szolgáltatást egy másik számítógépről, a szerverről kéri le a hálózat segítségével. A böngészők maguk is olyan kliensek, amelyek a webszerverekhez csatlakozva képesek megjeleníteni az egyes weboldalak tartalmát. A klienseknek három fajtája van:
– a *vastag kliens* (fat client) önállóan is képes működni anélkül, hogy csatlakozna egy szerverhez (asztali számítógép, notebook);
– a *vékony kliens* (thin client) nem képes szerver nélkül működni, saját funkciója csupán annyi, hogy grafikusan megjeleníti a szerverről érkező adatokat;
– a hibrid kliens képes önálló működésre, ugyanakkor adatbázisait a szerveren tárolja.

2 JTAG – Joint Test Action Group, az IEEE-1149.1 szabvány által meghatározott módszer az integrált áramköri lapok/rendszerek gyors és automatikus tesztelésére szolgál.

3 UART – Universal Asynchronous Receiver/Transmitter, olyan eszköz, amely jelátalakítást végez a soros és a párhuzamos interfészek között.

4 A hash-függvények (hasítófüggvények) informatikában használt eljárások, amelyek tetszőleges hosszúságú adatot rögzített hosszúságú, rövid kimenetbe (lenyomatba) képeznek.
A hasítófüggvények a számítástechnikában, az 1950-es évek elején jelentek meg, de az 1980-as évek végén, a digitális aláírás megjelenésével váltak szükségessé az informatikai biztonság érdekében. (A szerk.)