

Digitalna forenzika Android infotainment sistema u vozilu VW Golf 6: studija slučaja

Digital Forensics of an Android Infotainment System in a VW Golf 6: A Case Study

Adel Tahirović, Univerzitet Sinergija, Bijeljina

Sažetak — U ovom radu predstavljena je studija slučaja digitalne forenzike nad Android infotainment sistemom instaliranim u vozilu VW Golf 6. Digitalni dokazi prikupljeni su pomoću alata Android Debug Bridge (ADB). Zbog ograničenja unutar USB režima rada implementiranih od strane proizvođača, pristup uređaju ostvaren je putem bežičnog (wireless) protokola. Pokušaj integralne akvizicije podataka putem ADB protokola nije rezultirao validnom kopijom sistema, zbog čega se pristupilo selektivnom logičkom izuzimanju aplikacijskih artefakata, uključujući log zapise aplikacije Torque Pro. Pristup podacima ostvaren je putem On-Board Diagnostics (OBD-II) interfejsa, čime je omogućena direktna komunikacija sa elektronskim kontrolnim jedinicama (ECU) vozila preko Controller Area Network (CAN) magistrale. Dodatno su izuzeti podaci globalnog navigacionog satelitskog sistema (GNSS), generisani od strane Android infotainment sistema. Analizom CSV track-log zapisa rekonstruisana je vremenska linija kretanja vozila, procenjena pređena udaljenost i identifikovane faze mirovanja uz evaluaciju kvaliteta GNSS signala Horizontal Dilution of Precision (HDOP). Analiza potvrđuje da parcijalni artefakti Android infotainment sistema mogu imati značajnu dokaznu vrednost u rekonstrukciji događaja, uz jasno dokumentovana ograničenja akvizicije.

Ključne reči – digitalna forenzika; Android infotainment sistem; Android Debug Bridge (ADB); GNSS podaci; OBD-II/CAN komunikacija;

Abstract – This paper presents a digital forensic case study conducted on an Android-based infotainment system installed in a VW Golf 6 vehicle. Digital evidence was collected using the Android Debug Bridge (ADB) tool. Due to USB debugging restrictions implemented by the manufacturer, access to the device was gained through the wireless debugging method. A full ADB backup did not yield a usable copy of the data; therefore, a targeted logical extraction of available application artifacts was performed, including log records generated by the Torque Pro application. The analyzed logs contained data collected through OBD-II communication with the vehicle's ECU (CAN bus), as well as GNSS location data generated by the Android infotainment system. By analyzing CSV track log records, a timeline of the vehicle's movement was reconstructed, the traveled distance was estimated, and stationary phases were identified, along with an evaluation of GNSS signal quality (HDOP). The results demonstrate that even partially available artifacts from Android infotainment systems can have significant evidential value in reconstructing events, provided that the limitations of the acquisition process are clearly documented.

Keywords – digital forensics; Android infotainment system; Android Debug Bridge (ADB); OBD-II/CAN communication; GNSS data

I. UVOD

Savremena vozila integrišu veliki broj elektronskih kontrolnih jedinica, senzora i infotainment sistema koji generišu i pohranjuju podatke ključne za rekonstrukciju saobraćajnih nezgoda i izradu istražnih vremenskih linija [19]. Automobilaska digitalna forenzika definiše se kao proces pronalaženja, izdvajanja i interpretacije podataka iz modula vozila, mrežne komunikacije poput Controller Area Network (CAN) poruka i drugih ugrađenih sistema [16].

Budući da su infotainment sistemi danas standardni deo opreme, njihov značaj kao izvora dokaza postaje sve veći. Najčešće su to sistemi zasnovani na Android platformi, koji omogućavaju uvid u kretanje vozila, multimedijalni sadržaj i mrežnu povezanost [8]. Dosadašnja saznanja ukazuju na to da se istraživanja sve više usmeravaju na ove sisteme, ali se često zanemaruju praktična ograničenja prikupljanja podataka kada je konekcija putem USB veze na uređaju tvornički onemogućena [10]. Prethodno poznavanje forenzike mobilnih uređaja pruža osnovu, ali specifični hardverski restriktivni protokoli proizvođača automobila zahtevaju prilagođen pristup.

U ovoj studiji slučaja istraživao sam mogućnosti razvoja ponovljivog istraživačkog pristupa koji obuhvata:

(a) prikupljanje digitalnih dokaza sa Android infotainment sistema u uslovima ograničene konektivnosti, te

(b) kvantitativnu analizu Torque Pro log datoteka generisanih putem On-Board Diagnostics (OBD-II) komunikacije.

Fokusirao sam se na postupke provere integriteta podataka i dokumentovanje procesa akvizicije, nastojeći da jasno definišem metodološka ograničenja u skladu sa standardima rukovanja digitalnim dokazima [2].

II. TEORIJSKI OKVIR

Komunikacija između elektronskih sistema vozila najčešće se ostvaruje putem CAN magistrale, koja predstavlja standardizovanu tehnologiju za razmenu podataka unutar vozila definisanu standardom ISO 11898-1 [18]. CAN okvir sadrži identifikator poruke koji određuje prioritet komunikacije i pristup magistrali, što je od značaja i za inženjersku analizu i za forenzičku interpretaciju mrežnog saobraćaja [18].

Pristup dijagnostičkim podacima vozila ostvaruje se putem standardizovanog OBD-II 16-pinskog konektora, poznatog kao Data Link Connector (J1962 DLC).

Na ovom konektoru dostupne su različite komunikacione linije, uključujući CAN High i CAN Low, koje omogućavaju komunikaciju sa Electronic Control Unit (ECU) modulima vozila [17].

U praksi se za komunikaciju sa vozilom najčešće koriste OBD-II adapteri zasnovani na ELM327 arhitekturi, koji funkcionišu kao protokolarni prevodioci između mobilnih aplikacija i elektronskih sistema vozila [17]. Na aplikacionom nivou, podaci su adresirani preko standardizovanih OBD-II PID identifikatora definisanih standardom SAE J1979, koji omogućavaju pretvaranje sirovih bajtova odgovora iz ECU modula u fizičke veličine. Tipični primeri u forenzičkoj analizi su PID 0C (broj obrtaja motora), gde se vrednost dobija izrazom (1), i PID 0D (brzina vozila), definisan izrazom (2) [17]. Standardni PID primeri:

PID 0C (Engine RPM):

$$RPM = \frac{256A + B}{4} \quad (1)$$

Objašnjenje:

Ovaj izraz se koristi za interpretaciju odgovora na PID 0C. ECU vozila vraća dva bajta podataka, označena kao **A** (viši bajt) i **B** (niži bajt). Množenjem bajta A sa 256 vrši se pomeranje u 16-bitnom prostoru, dok se deljenjem sa 4 postiže rezolucija od 0,25 o/min, što je standard za OBD-II protokol [17]. U analiziranoj log-datoteci, ovaj parametar služi kao potvrda rada motora sa unutrašnjim sagorevanjem tokom zabeleženih Global Navigation Satellite System (GNSS) koordinata.

PID 0D (Vehicle speed):

$$\left[v_{\{OBD\}} \left(\frac{km}{h} \right) = A \right] \quad (2)$$

Objašnjenje:

Brzina vozila se dobija iz PID-a 0D. Za razliku od broja obrtaja motora (RPM), ovde se koristi samo jedan bajt (**A**), što znači da je maksimalna vrednost koju protokol može prijaviti 255 km/h. Važno je napomenuti da ova vrednost potiče direktno sa senzora na menjaču ili ABS prstenova točkova vozila VW Golf 6, te predstavlja 'unutrašnju' brzinu vozila koja može odstupati od 'spoljašnje' GNSS brzine usled faktora kao što su veličina pneumatika ili proklizavanje [20].

Za ekstrakciju podataka iz Android baziranih infotainment sistema koristi se Android Debug Bridge (ADB) protokol. ADB funkcioniše kao klijent-server arhitektura koja se sastoji od klijenta (forenzička radna stanica), servera i pozadinskog procesa (daemon) koji se izvršava na samom uređaju [21]. U kontekstu digitalne forenzike, ADB omogućava logičku akviziciju podataka putem komandne linije, čime se ostvaruje interakcija sa fajl-sistemom bez potrebe za modifikacijom hardvera [22].

Standardi digitalne forenzike naglašavaju potrebu očuvanja integriteta, revizionog traga i reproduktivnosti postupaka [2].

Standard ISO/IEC 27037 definiše procese identifikacije, prikupljanja i očuvanja digitalnih dokaza, dok smernice organizacija poput NIST-a i SWGDE naglašavaju minimalnu izmenu originalnih podataka i detaljno dokumentovanje procesa analize [3].

III. MATERIJALI I METODE

Predmet istraživanja bio je Android infotainment sistem instaliran u vozilu VW Golf 6 čije su detaljne tehničke specifikacije i forenzički parametri prikazani u tabeli 1. Cilj analize bio je utvrditi da li je moguće rekonstruisati vremensku liniju kretanja vozila na osnovu aplikacionih artefakata generisanih tokom vožnje [10].

Podaci su generisani koristeći aplikaciju Torque Pro, koja je bila povezana sa vozilom putem ELM327 OBD-II adaptera [1]. Radi očuvanja integriteta podataka izračunate su Secure Hash Algorithm 256-bit (SHA-256) kriptografske hash vrednosti za sve izdvojene digitalne artefakte, prikazane u tabeli 2 [2].

Inicijalni pokušaji direktnog fizičkog povezivanja putem USB režima rada nisu dali rezultate usled restriktivnih sigurnosnih politika proizvođača. Razmatrana je i metoda fizičke ekstrakcije podataka direktno sa memorijskog čipa (*chip-off*), ali je ona odbačena zbog rizika od trajnog uništenja hardvera i narušavanja integriteta sistema u ovoj fazi istrage. Shodno tome, kao primarna metoda za akviziciju podataka odabrano je bežično (wireless) povezivanje. U forenzičkom kontekstu, ovakav pristup se klasifikuje kao udaljena logička akvizicija (eng. remote logical acquisition), jer kanal pristupa nije neposredni fizički medij, već mrežna infrastruktura koja zahteva uparivanje i autorizaciju [11]. Bilo je neophodno detaljno dokumentovati svaki korak uspostavljanja veze uključujući, mrežni interfejs, logički identitet radne stanice i tačno vreme svake akcije kako bi se osigurao potpun reviziono trag i minimizovao rizik od nenamernih izmena na uređaju.

TABELA 1. TEHNIČKI I FORENZIČKI KONTEKST ANALIZIRANOG UREĐAJA

Parametar	Vrednost
Vozilo	VW Golf 6
Tip uređaja	Android infotainment sistem u vozilu
Operativni sistem	Android 11
Build verzija	V1.07.10-20250629
Način pristupa	Wireless debugging (ADB)
Root pristup	Nije dostupan
USB ADB pristup	Ograničen / nije omogućio potpunu akviziciju
Pokušaj ADB full backup-a	Izvršen, ali nije dao upotrebljiv rezultat
Tip akvizicije	Ciljano logičko izdvajanje podataka
Relevantna aplikacija	Torque Pro ver. 1.12.108
Korišćeni adapter	ELM327 ver. 1.5
Izvor analiziranih podataka	OBD-II/CAN komunikacija i GNSS zapisi aplikacije
Izdvojeni artefakti	CSV log, bugreport/dumpstate, ADB backup artefakt

Dokazni paket je sadržao: (1) Torque Pro export u ZIP formatu, (2) CSV track log kao primarni analitički artefakt, (3) sistemski dijagnostički izveštaj (bugreport/dumpsys), te (4) ADB full_backup artefakt koji je ukazivao na neuspešan pokušaj potpunog izvlačenja sigurnosne kopije iz uređaja.

TABELA 2. DIGITALNI ARTEFAKTI I SHA-256 VREDNOSTI ZA PROVERU INTEGRITETA

Artefakt	Veličina (bytes)	SHA-256
dumpsys_detalji.txt	13859517 bytes	34a30c6237bfe28972b93859db82ceb78bda3adf48be2d907da931ce173a5cd
trackLog-2026-Mar-02_19-30-20.csv	713614 bytes	a70c149bcd347b96046042735f49fb77f87329a3b0d2754abb3f90c99edc543
zipExport-2026-03-02_19-38-48.zip	43509 bytes	7975c754c0fba980d404ca5aa597be2a00a3b848cb22a3309ba213744ac4c9f
full_backup.ab	0 bytes	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Izračunavanje kriptografskih hash vrednosti predstavlja standardnu proceduru u digitalnoj forenzici, jer omogućava verifikaciju integriteta digitalnih dokaza između faze akvizicije i faze analize. Ukoliko se hash vrednost artefakta promeni, to ukazuje na potencijalnu izmenu podataka.

IV. REZULTATI

Analiza izdvojene datoteke trackLog.csv rezultovala je identifikacijom preko 90 različitih dijagnostičkih, lokacionih i sistemskih parametara koji su beleženi u realnom vremenu. Za potrebe forenzičke rekonstrukcije događaja, iz bogatog skupa podataka izvršena je ciljana selekcija varijabli koje omogućavaju precizno mapiranje kretanja i stanja vozila:

Vremensko-lokacioni parametri: GPS Time, Latitude i Longitude poslužili su kao osnova za hronološko mapiranje kretanja.

Dijagnostički parametri vozila (OBD-II): Engine RPM (broj obrtaja) i Speed (OBD) odabrani su kao primarni indikatori rada motora i mehaničkog kretanja vozila, dok su parametri poput *Throttle Position* (položaj pedale gasa) korišćeni za analizu ponašanja vozača.

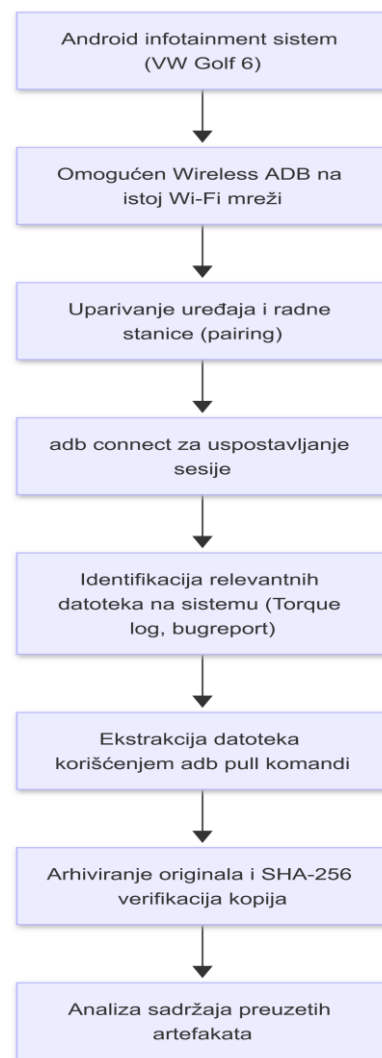
Metapodaci validacije: Horizontal Dilution of Precision (HDOP) i GPS Satellites ekstrahovani su radi evaluacije pouzdanosti lokacionih podataka, što je ključno za forenzičku verifikaciju preciznosti zapisa.

Klasifikacija ovih podataka omogućila je formiranje korelacionog modela između unutrašnjih senzora vozila i eksternih GNSS podataka, čime je potvrđen integritet celokupne vožnje. Tabela 3 prikazuje pregled ključnih ADB naredbi korišćenih tokom postupka akvizicije digitalnih artefakata sa Android infotainment sistema.

TABELA 3. PREGLED KLJUČNIH ADB NAREDBI KORIŠĆENIH U PROCESU AKVIZICIJE PODATAKA

ADB naredba	Opis operacije	Svrha u forenzičkom procesu
adb pair 192.168.1.15:37445842931	Uparivanje uređaja sa radnom stanicom	Autentifikacija i dozvola pristupa sistemu
adb connect 192.168.1.15:41029	Uspostavljanje aktivne mrežne sesije	Kreiranje kanala za prenos digitalnih dokaza
adb shell bugreport > b.zip	Generisanje sveobuhvatnog izveštaja	Ekstrakcija sistemskih log datoteka i dijagnostike

Celokupan operativni postupak akvizicije strukturiran je kao forenzički tok obrade dokaza, koji je precizno definisan i vizuelno predstavljen na slici 1.



Sl.1 Dijagram toka procesa bežične akvizicije podataka sa Android infotainment sistema

Primenjeni model sa slike 1 podrazumeva identifikaciju relevantnih izvora podataka (dnevnički zapisi aplikacija, datoteke izvoza podataka, privremene datoteke) i njihovo

izdvajanje uz minimalnu izmenu originalnog sadržaja [2]. Proces obuhvata sledeće ključne faze:

1. identifikaciju relevantnih digitalnih artefakata.
2. izradu forenzičke kopije dostupnih podataka.
3. izračunavanje kriptografskih hash vrednosti radi provere integriteta.
4. očuvanje originalnih datoteka u read-only režimu.
5. analizu podataka nad verifikovanim kopijama artefakata.

Ovakav pristup je u potpunosti u skladu sa preporukama standarda ISO/IEC 27037 i smernicama organizacije SWGDE za rukovanje digitalnim dokazima [2].

V. ANALIZA I TUMAČENJE IZDOJENIH ARTEFAKATA

Analiza je bila usmerena na rekonstrukciju kretanja vozila na osnovu podataka track log zapisa aplikacije Torque Pro. Skup podataka je sadržavao 1513 uzoraka u vremenskom periodu od približno 45 minuta i 29 sekundi. Prosečni interval uzorkovanja bio je oko jedne sekunde. Ovakav način uzorkovanja je u skladu sa tipičnim načinom rada aplikacija za praćenje vožnje, gde se podaci beleže u kratkim vremenskim intervalima, ali može doći do povremenih prekida usled gubitka GNSS signala ili promena stanja aplikacije [20].

Za procenu udaljenosti između uzastopnih GNSS koordinata korišćena je haversine formula definisana jednačinom (4), koja omogućava izračunavanje udaljenosti između dve tačke na površini Zemlje na osnovu njihove geografske širine i dužine [20]. Pošto GNSS koordinatni zapisi koriste vrednosti izražene u stepenima, neophodno je izvršiti njihovu konverziju u radijane prema jednačini (3).

Jednačina za pretvaranje stepeni u radijane:

$$\varphi(\text{rad}) = \varphi(\text{deg}) \cdot \frac{\pi}{180} \quad (3)$$

Jednačina za izračunavanje udaljenosti između dve GNSS tačke definisana je sledećim izrazom:

$$d = 2R \arcsin \left(\sqrt{\sin^2\left(\frac{\Delta\varphi}{2}\right) + \cos(\varphi_1)\cos(\varphi_2)\sin^2\left(\frac{\Delta\lambda}{2}\right)} \right) \quad (4)$$

gde su:

- **R** – radijus Zemlje (približno 6371 km)
- **φ_1 i φ_2** – geografske širine dve GNSS tačke
- **λ_1 i λ_2** – geografske dužine dve GNSS tačke
- **$\Delta\varphi$** – razlika geografskih širina između dve tačke
- **$\Delta\lambda$** – razlika geografskih dužina između dve tačke
- **d** – udaljenost između dve GNSS pozicije.

Na osnovu izračunate udaljenosti između uzastopnih GNSS koordinata i vremenskog intervala između uzoraka moguće je proceniti trenutnu brzinu kretanja vozila [20]. Procena brzine može se izračunati pomoću sledeće jednačine (5):

$$v = \frac{\Delta d}{\Delta t} = \frac{(d_2 - d_1)}{t_2 - t_1} \quad (5)$$

gde je:

- **v** – procenjena brzina kretanja vozila
- **Δd** – udaljenost između dve uzastopne GNSS pozicije
- **Δt** – vremenski interval između dva uzorka.

S obzirom na to da su sirovi podaci u log-datoteci aplikacije Torque Pro za parametar GPS Speed izraženi u metrima po sekundi (m/s), izvršena je konverzija u kilometre na čas (km/h) primenom sledeće jednačine (6):

$$\frac{v_{km}}{h} = \frac{v_m}{s} \cdot 3,6 \quad (6)$$

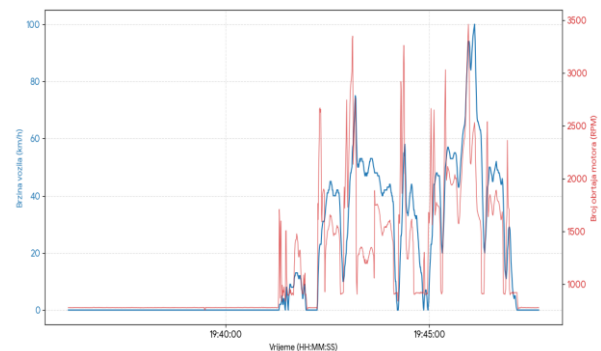
Ova transformacija je neophodna radi standardizacije prikaza rezultata i lakše korelacije sa brzinom očitane putem OBD-II interfejsa vozila [17]. Primenom navedenog matematičkog modela nad verifikovanim skupom podataka, dobijeni su sledeći rezultati kretanja:

- ukupna pređena udaljenost: 14,39 km
- prosečna brzina vozila: 26,95 km/h
- maksimalna zabeležena brzina: 64,12 km/h

Analiza distribucije brzine pokazala je da je približno 20,36% uzoraka imalo vrednost manju od 1 km/h, što ukazuje na faze mirovanja (stajanje na semaforima, raskrsnicama ili parkiranje).

A. Forenzička korelacija i validacija podataka

Ključni aspekt analize artefakata je potvrda autentičnosti zapisa korelacijom različitih senzora. U digitalnoj forenzici vozila, podudaranje rada motora sa kinetikom vozila služi kao dokaz da podaci nisu naknadno manipulisani ili generisani greškom softvera.

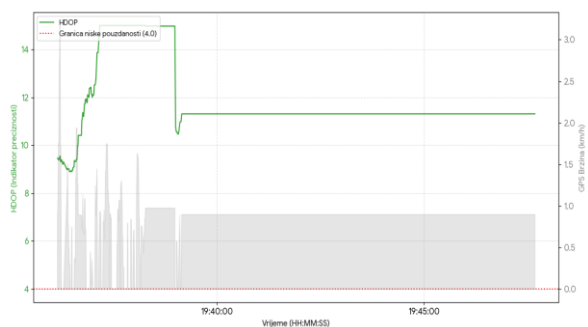


Sl.2 Korelacija brzine kretanja vozila (OBD) i broja obrtaja motora (RPM)

Podaci na slici 2 pokazuju visoku koherentnost: svaki porast broja obrtaja motora (RPM) korelira sa promenom brzine očitane preko OBD-II interfejsa. Ovakva podudarnost potvrđuje da je Android infotainment sistem ispravno procesuirao podatke dobijene putem aplikacije i ELM327 adaptera sa CAN magistrale vozila u realnom vremenu [18].

B. Analiza pouzdanosti GNSS signala

Pored kinetičkih parametara, analiziran je i Horizontal Dilution of Precision (HDOP) parametar kao primarni indikator kvaliteta geolokacijskih podataka. Niže vrednosti HDOP-a ukazuju na bolju geometriju satelita i veću preciznost, dok visoke vrednosti sugerišu povećanu marginu greške.



SI.3 Analiza pouzdanosti GNSS signala (HDOP) i brzine kretanja

U analiziranom skupu podataka, HDOP vrednosti su varirale između 1,7 i 15. Kao što je prikazano na slici 3, određeni segmenti vožnje karakterišu se HDOP vrednostima iznad kritične granice od 4,0, što ukazuje na periode smanjene forenzičke pouzdanosti. Ovi ekstremi su verovatno uzrokovani ambijentalnim faktorima poput urbanih kanjona ili drvoreda koji ometaju direktnu vidljivost GNSS satelita.

C. Analiza strukture ekstrahovanih podataka

Detaljnim pregledom ekstrahovane datoteke utvrđeno je da sistem beleži preko 30 senzorskih parametara. Za potrebe istraživanja, kao primarni markeri izdvojeni su: GPS Time, Latitude, Longitude, GPS Speed, HDOP i Engine RPM. Posebna pažnja posvećena je koloni Device Time. Njeno prisustvo omogućava forenzičku proveru eventualnog odstupanja između sistemskog sata Android infotainment sistema i atomskog vremena dobivenog putem GNSS-a. U analiziranim uzorcima uočena je potpuna sinhronizacija, što olakšava precizno smeštanje događaja u vremensku liniju istrage.

Na osnovu rezultata možemo potvrditi da, uprkos ograničenjima poput povremenih prekida u zapisu ili varijabilne preciznosti signala, artefakti iz Android infotainment sistema predstavljaju robustan izvor dokaza [10]. Za maksimalnu naučnu sigurnost, preporučuje se da se ovi podaci uvek interpretiraju uz uvažavanje HDOP indikatora i, gde je moguće, potvrde eksternim izvorima poput ECU log datoteke ili telemetrije.

VI. DISKUSIJA

Rezultati studije slučaja potvrđuju da Android infotainment sistemi predstavljaju izuzetno relevantan izvor digitalnih dokaza u automobilskim istragama, naročito kada se zahteva precizna rekonstrukcija vremenske linije kretanja, analiza obrasca brzine i identifikacija faza mirovanja vozila [10]. Temeljni dokazni materijal u ovom istraživanju zasnovan je na log-datoteci aplikacije Torque Pro, pomoću koje je izvršena detaljna kvantitativna rekonstrukcija kretanja u trajanju od oko 45 minuta. Takav tip artefakta je praktično vredan jer se često

može pribaviti i u uslovima kada je potpuna fizička akvizicija ograničena ili tehnički neizvodiva [11].

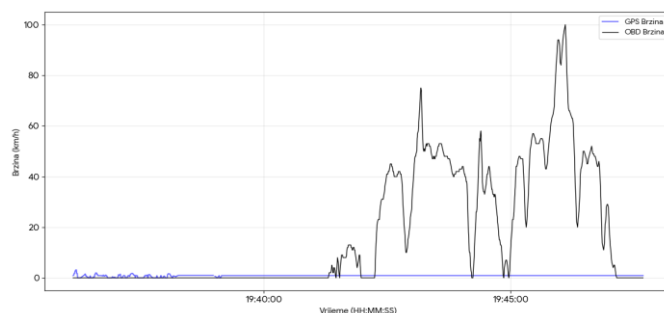
Ipak, interpretacija zapisa zasnovanih na GNSS tehnologiji mora ostati forenzički konzervativna [20]. Prvo, kvalitet GNSS signala varira u zavisnosti od okruženja (urbani kanjoni, tuneli, drvoređi), što može dovesti do povećanih grešaka pozicioniranja [20]. Zbog toga je parametar HDOP ključan indikator nesigurnosti: niže vrednosti tipično impliciraju bolju geometriju satelita i manju horizontalnu grešku, dok više vrednosti ukazuju na slabiju pouzdanost lokacijskog podatka [20]. U kontekstu digitalne forenzike, to znači da se segmenti sa povećanim HDOP vrednostima ne bi smeli koristiti za precizne tvrdnje o apsolutnoj lokaciji bez dodatne potvrde, već prvenstveno za prepoznavanje opšteg obrasca kretanja [2].

Drugo, prisutni prekidi u logovanju (time gaps) uvode rizik da kumulativna udaljenost izračunata haversine formulom potcenjuje realnu pređenu udaljenost, jer se preskaču segmenti između dve zabeležene tačke. Iz tog razloga, preporučuje se da se prekidi eksplicitno označe u rezultatima (npr. broj prekida dužih od 10 s i maksimalna pauza), te da se u diskusiji naglasi da su takvi intervali empirijski „nepoznati“, a ne interpolirani [2].

Treće, ključni doprinos rada je detaljno dokumentovanje ograničenja akvizicije: USB komunikacija je bila onemogućena od strane proizvođača, pa je pristup ostvaren putem metode bežičnog debugovanja (wireless debugging), dok je pokušaj kreiranja potpune ADB sigurnosne kopije sistema rezultovao praznom datotekom. Takva ograničenja su tipična za savremene infotainment sisteme, gde proizvođači primenjuju ograničenja pristupa sistemskim interfejsima, a novije verzije Android operativnog sistema dodatno ograničavaju generičke mehanizme sigurnosne kopije [10]. Iz forenzičke perspektive, to zahteva jasnu distinkciju između:

- (a) podataka koji su bili dokazno dostupni i analizirani i
- (b) podataka koji bi potencijalno postojali, ali nisu mogli biti prikupljeni u datim uslovima.

U dobroj praksi, ova distinkcija se jasno navodi u metodologiji i diskusiji, kako bi zaključci bili zasnovani isključivo na stvarno prikupljenim i verifikovanim artefaktima. Preporučuje se metodološka triangulacija izvora podataka gde god je moguća: korelacija dnevničkih zapisa infotainment sistema sa nezavisnim izvorima kao što su ECU log datoteke ili drugim vremenski sinhronizovanim izvorima lokacijskih podataka [3].



SI.4 Komparativna analiza GPS i OBD brzine vozila (Validacija podataka)

Takva korelacija, prikazana na slici 4, može dodatno ojačati dokaznu vrednost istraživanja i značajno smanjiti nesigurnost, posebno u segmentima sa slabijim GNSS kvalitetom ili prekidima u evidentiranju podataka [2].

VII. ZAKLJUČAK

Ovaj rad predstavlja studiju slučaja digitalne forenzike nad Android infotainment sistemom instaliranim u vozilu VW Golf 6. Sa primarnim fokusom na metodologiju izdvajanja i analize podataka, istraživanje je pokazalo da savremena vozila predstavljaju kompleksne digitalne ekosisteme čiji artefakti mogu biti od presudnog značaja za forenzičku rekonstrukciju događaja.

Zbog implementiranih ograničenja USB ADB komunikacije i neuspešnog pokušaja kreiranja potpunog backup-a (potpune sigurnosne kopije) uređaja, proces akvizicije uspešno se oslonio na metodu bežičnog debugovanja (Wireless debugging) i ciljano logičko izvlačenje aplikacionih artefakata. Analizom dnevnčkih zapisa (track log) aplikacije Torque Pro, precizno je rekonstruisana vremenska linija kretanja vozila u trajanju od približno 45 minuta, uz procenu pređene udaljenosti od 14,39 km i jasnu identifikaciju perioda mirovanja.

Korelacija dobijenih rezultata putem komparativne analize brzine i broja obrtaja motora potvrdila je integritet i autentičnost izuzetih digitalnih dokaza. Rezultati istraživanja nedvosmisleno potvrđuju da Android infotainment sistemi predstavljaju vredan izvor podataka u automobilskim istragama, čak i u scenarijima u kojima je dostupna samo parcijalna akvizicija. Ključ uspešne forenzičke obrade leži u preciznom dokumentovanju procesa, verifikaciji integriteta putem kriptografskih hash vrednosti i kritičkom uvažavanju ograničenja preciznosti GNSS signala.

Buduća istraživanja trebalo bi da se usmere na automatizaciju korelacije između artefakata dobijenih iz Android infotainment i podataka iz drugih elektronskih kontrolnih jedinica vozila (ECU) radi postizanja još većeg stepena forenzičke sigurnosti.

LITERATURA

- [1] A. Årnes, Ed., *Digital Forensics: An Academic Introduction*. Hoboken, NJ: Wiley, 2018.
- [2] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Waltham, MA: Academic Press, 2011.
- [3] E. Casey, *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press, 2009.
- [4] J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, 2nd ed. Waltham, MA: Syngress/Morgan Kaufmann, 2015.
- [5] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th ed. Boston, MA: Cengage, 2019.
- [6] N. A. Hassan, *Digital Forensics Basics: A Practical Guide Using Windows OS*. Berkeley, CA: Apress, 2019.
- [7] B. Carrier, *File System Forensic Analysis*. Boston, MA: Addison-Wesley Professional, 2005.
- [8] A. Hoog, *Android Forensics: Investigation, Analysis, and Mobile Security for Google Android*. Waltham, MA: Syngress, 2011.
- [9] O. Skulkin, D. Tindall, and R. Tamma, *Learning Android Forensics*, 2nd ed. Birmingham, U.K.: Packt Publishing, 2018.
- [10] R. Tamma, O. Skulkin, H. Mahalik, and S. Bommisetty, *Practical Mobile Forensics: Forensically Investigate and Analyze iOS, Android, and Windows 10 Devices*, 4th ed. Birmingham, U.K.: Packt Publishing, 2020.
- [11] L. Reiber, *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*, 2nd ed. New York, NY: McGraw-Hill Education, 2019.
- [12] C. Easttom, *An In-Depth Guide to Mobile Device Forensics*. Boca Raton, FL: CRC Press, 2022.
- [13] J. Bair, *Seeking the Truth from Mobile Evidence: Basic Fundamentals, Intermediate and Advanced Overview of Current Mobile Forensic Investigations*. Cambridge, MA: Academic Press, 2017.
- [14] I. I. Androulidakis, *Mobile Phone Security and Forensics: A Practical Approach*, 2nd ed. Cham: Springer, 2016.
- [15] A. Gehlot, R. Singh, J. Singh, and N. R. Sharma, Eds., *Digital Forensics and Internet of Things: Impact and Challenges*. Hoboken, NJ: Wiley, 2022.
- [16] S. Kim and R. Shrestha, *Automotive Cyber Security: Introduction, Challenges, and Standardization*. Singapore: Springer, 2020.
- [17] C. Smith, *The Car Hacker's Handbook: A Guide for the Penetration Tester*. San Francisco, CA: No Starch Press, 2016.
- [18] W. Lawrenz, Ed., *CAN System Engineering: From Theory to Practical Applications*, 2nd ed. London: Springer, 2013.
- [19] D. P. F. Möller and R. E. Haas, *Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications*. Cham: Springer, 2019.
- [20] E. D. Kaplan and C. Hegarty, Eds., *Understanding GPS/GNSS: Principles and Applications*, 3rd ed. Norwood, MA: Artech House, 2017.