Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Automatizace forenzního zkoumání navigačních zařízení

Bakalářská práce

Adam Pokorný

Vedoucí práce: Ing. Jaroslav Kothánek, Ph.D.

České Budějovice 2017

Bibliografické údaje

Pokorný A., 2017: Automatizace forenzního zkoumání navigačních zařízení.

[Automation of Forensic Examining – navigation devices. Bc. Thesis, in Czech] - 39 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Tato bakalářská práce se zabývá forenzní analýzou souborů z obrazu disku GPS přístrojů. Cílem je vytvoření nástroje, který bude schopný automaticky zanalyzovat a vypsat dostupné informace.

Abstract

This bachelor thesis deals with the forensic analysis of files from a GPS memory image. The goal is to provide a tool that is able to automatically analyze and show available information.

Klíčová slova

GPS, bitová kopie, obraz, disk, analýza, hardware, software, program, forenzní zkoumání

Keywords

GPS, image, hard drive, analysis, hardware, software, forensic analysis, examining

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG, provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz, provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 2.12. 2017

……

Poděkování

Rád bych poděkoval svému vedoucímu práce Ing. Jaroslavu Kothánkovi, Ph.D.

za trpělivost a důvěru.

Obsah

ÚVOD

Již od počátku lidstva hnala touha cestovat a objevovat skupinky dobrodruhů na cesty po tehdy známém i neznámém světě. Vývoj navigačních systému byl tlačen kupředu nutností orientovat se v prostředí, i přes to se však nové nápady objevovali velice pomalým tempem. Systémů, jak se orientovat - od orientačního bodu v podobě zapamatovatelného místa, určování trasy pomocí hvězd, odhadnutí polohy na mapě, zaměření pomocí sextantu, až po dnešní technologie GPS - bylo v historii lidstva mnoho. [1]

Nikdy však neexistovala přesnější a pro uživatele jednodušší možnost, jak zjistit svou polohu a najít správnou cestu. Na rozdíl však od metod předcházejících, GPS pro své správné fungování potřebuje velice nákladné a složité přípravy. Tento systém je postaven na činnosti soustavy navigačních družic, obíhajících Zemi, poskytujících celosvětové autonomní určování polohy. Každý uživatel musí mít malý rádiový přijímač, který na základě přijímaných signálů z družic umožní vypočítat svou polohu s přesností na desítky až jednotky metrů.

Tyto malé rádiové přijímače jsou většinou nastaveny tak, aby do své paměti po určitých časových intervalech ukládali svůj čas, nadmořskou výšku, zeměpisnou šířku a zeměpisnou délku. Z těchto dat lze zpětně zjistit velké množství konkrétních informací, které nám mohou pomoci odpovědět na naše otázky.

Pokud potřebujeme zjistit kde, v jakou dobu a jakou rychlostí se určitý přijímač pohyboval, můžeme využít dříve zmiňovaných dat a údaje z přístroje dostat. Tuto možnost často využívá policie nebo soudní znalci. Zkoumání GPS přístrojů pro tyto potřeby je však velmi zdlouhavé, proto přichází nutnost automatizace za pomocí programu.

MOTIVACE

Při vyšetřování některých trestných činů je nutné vědět, kde a v jaký čas se určitý člověk pohyboval. Ať už se jedná o nevěru nebo těžký zločin, dá se pro zjištění těchto informací využít mnoho různých technik. Od slovní výpovědi, záznamu z kamer, až po využití automaticky ukládaných dat v GPS přístroji. Většinou stačí, aby byla v inkriminovanou dobu GPS zapnuta a potřebná data se zaznamenávají do paměti, aniž by o tom kdokoliv věděl.

Způsobů, jak se k daným informacím dostat, je více. Nejjednodušší možností je se podívat přímo do spuštěného GPS přístroje, což je ale nepoužitelné u soudu kvůli zásadám forenzní analýzy. Další možností je vytěžení informací ručně, což je značně pomalé. Možností nejlepší je použití již existujícího softwaru. Program, který však splňuje legislativní postupy a je zdarma, v současné době neexistuje.

CÍLE PRÁCE

Cílem práce je vytvoření programu v OS Linux pro analýzu GPS přijímačů. Tento program načte bitovou kopii paměti z GPS a zkusí automaticky vytěžit veškerá dostupná data zahrnující typ zařízení, verze map, domov a další oblíbená uložená místa, všechny projeté trasy včetně rychlosti v konkrétních bodech a času. První možnost bude údaje rovnou zobrazit v přehledné formě v okně programu. Druhou možností bude vytvoření reportu, který bude dostupný ve formátu *.pdf*. Vytvořený program bude později implementován do live distribuce. K závěru zhodnotím přínos, užitečnost a použitelnost programu pro policii a soudní znalce.

1 FORENZNÍ ANALÝZA VÝPOČETNÍ TECHNIKY - POSTUPY PŘI ZAJIŠŤOVÁNÍ A VYHODNOCOVÁNÍ DAT

1.1 DIGITÁLNÍ FORENZNÍ ANALÝZA

„Digitální forenzní analýza (DFA) je věda a zároveň i umění toho, jak zajišťovat, hledat a vytěžovat digitální data pro specifické účely. Tato data mohou být důkazem spáchání trestného činu, mohou potvrzovat nebo vyvracet porušení interních předpisů nebo to mohou být prostě důležité informace, které jsou pro klienta běžným způsobem nedostupné.“ [2]

DFA patří do velké rodiny forenzních věd. *„Forenzní vědy jsou vědy, které se zabývají vývojem a aplikací specifických metod na vědeckém základě, které napomáhají při vyšetřování a dokazování trestných činů*.“ [3]

Do této skupiny patří mnoho dalších známých oborů, jako například forenzní balistika, forenzní chemie, forenzní medicína či forenzika fotografií. Patří sem ale i méně známá analýza otisku ucha, forenzika leteckých snímků, forenzní meteorologie a další.

V dnešní době má DFA uplatnění všude tam, kde se můžeme setkat s různými druhy trestního nebo jiného protiprávního jednání. Ve většině případů se zde totiž můžeme setkat i s digitálními informacemi, ať už ve formě počítače, mobilu nebo dnes i paměti v automobilu a jiné.

1.2 ZÁSADY ZKOUMÁNÍ DIGITÁLNÍCH DAT

Aby se výsledky bádání dali použít jako důkaz (v právním slova smyslu), musí analýza digitálních dat splňovat obecné vlastnosti forenzního zkoumání.

1) Legalita - tj. veškeré informace, předměty, zdroje, vstupy a výstupy atp., musí být získány a zhotoveny legálním způsobem. To znamená využití legálně koupeného softwaru, legálně získaných důkazů a neporušit zákony, které s naším zkoumáním mohou potencionálně kolidovat (telekomunikační zákon, zákon na ochranu osobních údajů a jiné).

2) Integrita - tj. veškeré manipulování se vstupními informacemi musí být prováděno takovým způsobem, aby bylo jednoznačně jasné, že nemohlo dojít k úmyslné či neúmyslné změně zkoumaných dat. Většinou se využije bitová kopie média či read-only mód.

3) Opakovatelnost / přezkoumatelnost - tj. dělat analýzu a její dokumentaci takovým způsobem, aby se zajistila možnost dojít ke stejným výsledkům opakováním použitých metod.

4) Nepodjatost - tj. nezávislost subjektu pověřeného forenzní činností na zkoumaném předmětu nebo objektu.

5) Detailní dokumentace - tento bod podmiňuje všechny předešlé. Bez dobré dokumentace by bylo velice obtížné prokázat závěry, ale dokázat i splnění výše uvedených atributů.

2 GLOBAL POSITIONING SYSTEM

„Global Positioning System, zkráceně GPS, je vojenský navigační družicový systém provozovaný Ministerstvem obrany Spojených států amerických, který dokáže s několikametrovou přesností určit pozici kdekoliv na Zemi. Přesnost GPS lze ještě zvýšit až na přibližně 1 cm s použitím metod jako je Diferenciální GPS (DGPS).“ [1] Kromě určení geografické polohy měří tento systém také čas, přesnost se pohybuje v jednotkách nanosekund.

2.1 HISTORIE

Celý projekt navazuje na předchozí GNSS Transit, jenž byl historicky první družicový polohový systém (1964-1996) provozovaný námořnictvem USA. Jeho technologie dovolovaly určovat polohu s přesností na stovky metrů a přesný čas kdekoliv na Zemi.

GPS (dříve NAVSTAR GPS - Navigation Signal Timing and Ranging Global Positioning System) tento projekt rozšiřuje o kvalitu, dostupnost, přesnost a služby. Vývoj začal v roce 1973 sloučením dvou projektů, System 621B pro určování polohy a projekty Timation pro přesné určování času.

Od let 1978-1985 začalo vypouštění 11 vývojových družic a později roku 1979 byl rozšířen plán z nedostačujících 18 družic na 24. [4]

Přelom pro použití pro civilní obyvatelstvo nastal v roce 1983, kdy sovětská stíhačka sestřelila civilní linkový let Korean Air 007, který se chybou posádky odchýlil ze své původní trasy o 200mil a vletěl do sovětského vzdušného prostoru. Kvůli této události byla zatím tajná technologie GPS prezidentem Ronaldem Reaganem odtajněna a uvolněna pro civilní použití, aby se podobným tragickým omylům předešlo. [5]

2.2 SEGMENTY GPS

GPS tvoří tři segmenty - kosmický, kontrolní a uživatelský. Kosmická část je tvořena družicemi na oběžné dráze, kontrolní segment zahrnuje pozemní řídící a vysílací stanice. Uživatelský segment tvoří přijímače GPS.

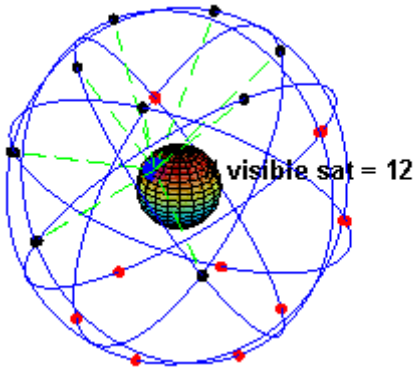
2.2.1 KOSMICKÝ SEGMENT

Kosmický segment je tvořen minimálně 24 družicemi. Reálný počet je ale proměnlivý, jsou totiž vyráběny a vypouštěny stále nové generace družic a staré se vypínají až podle technického stavu. V dnešní době je využíván mezní počet 32 družic.

Družice jsou umístěny na šesti téměř kruhových drahách se sklonem 55 stupňů k rovině rovníku, vzdálenost od povrchu Země je 20 350 km a pohybují se rychlostí 11 300 km/h.

Součástí každé družice je přijímač, vysílač, atomové hodiny, procesory a ostatní přístroje sloužící nejen pro navigaci (např. detekce atomových výbuchů a jiných vojenských účelů). Družice také přijímá, zpracovává a uchovává informace předané pozemními anténami.

Družice sama sleduje stav vlastních systémů a koriguje svojí dráhu raketovými motory. O stabilizaci na dráze se starají setrvačníky a o dobíjení palubních baterií sluneční články.

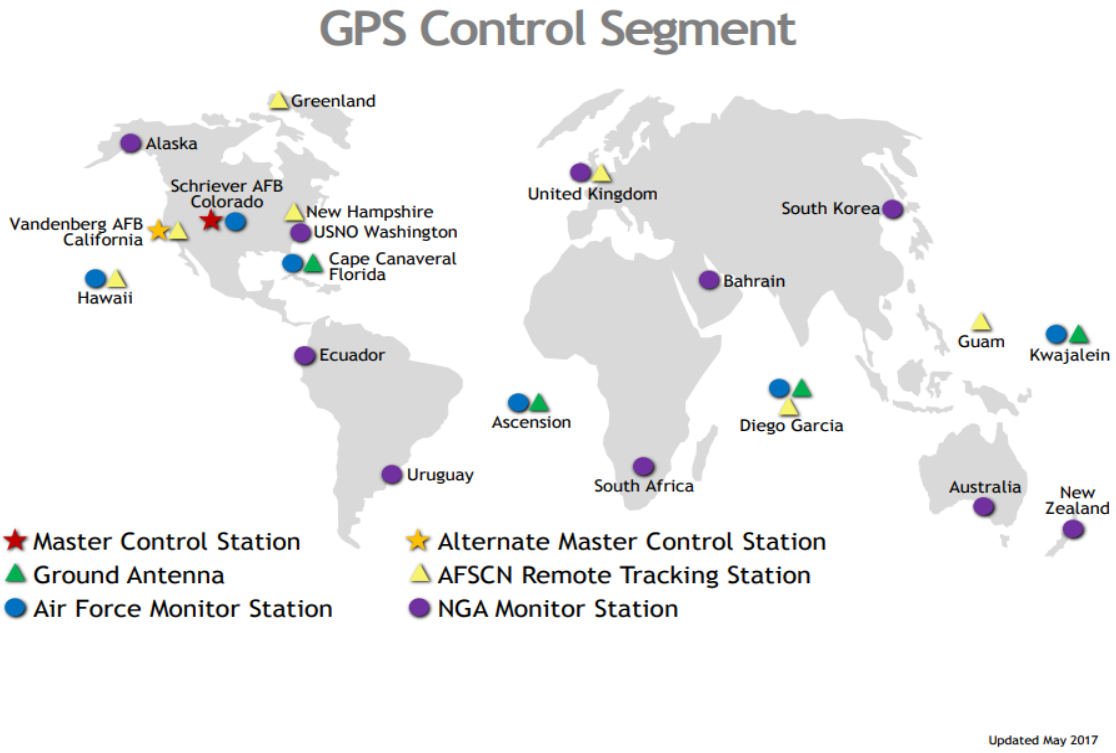


Obrázek 1 - konstelace GPS

[https://cs.wikipedia.org/wiki/Global_Positioning_System#/media/File:ConstellationGPS.gif]

2.2.2 ŘÍDÍCÍ SEGMENT

Tento segment se skládá z velitelství, řídícího střediska, 3 povelových stanic a 18 monitorovacích stanic. Úkolem řídícího a kontrolního segmentu je monitorovat segment kosmický, zasílat družicím potřebné povely a provádět manévry a údržbu atomových hodin.



Obrázek 2 - kontrolní segment GPS

[https://www.gps.gov/multimedia/images/GPS-control-segment-map.pdf]

2.2.3 UŽIVATELSKÝ SEGMENT

Uživatelský segment je tvořen pasivními GPS přijímači, které přijímají signály z jednotlivých družic. Z přijatých dat přijímač vypočítá polohu antény, nadmořskou výšku a přesné datum a čas.

V dnešní době existuje nepřeberné množství typů a značek přijímačů a právě jejich analýzou se v této práci zabývám.

3 METODIKA ZKOUMÁNÍ

3.1 BITOVÁ KOPIE PAMĚTI

Analyzována bude bitová kopie paměťového média v GPS přijímači. Tato kopie je naprosto identická jako její originální vzor, včetně potencionálních, dříve uskutečněných, modifikací a úprav.

Pro vytvoření bitové kopie se dá využít mnoho volně šiřitelných programů, které existují pod většinou operačních systémů. Například na Linuxu je asi nejznámějším program „dd“.

Bitovou kopii musí program načíst jako read-only (pouze pro čtení), jinak by mohla být narušena jedna ze zásad forenzní analýzy - integrita.

3.2 ZÍSKÁNÍ DAT

Místa, kde budeme hledat data, která potřebujeme (domov, oblíbená uložená místa, trasy, časy uložení a jiné) se liší od výrobce k výrobci. Obecně se ale budeme poohlížet po XML a textových souborech, které obsahují veškerá námi vyžadovaná data. Naneštěstí, velké množství výrobců využívá svůj vlastní formát dat, ve kterém informace ukládá.

3.2.1 GARMIN

Navigace Garmin ukládá cestovní data do formátu *.gpx*, což je specifické XML schéma, které je volně čitelné v paměti navigačního přístroje. Formát *.gpx* (the GPS eXchange Format) je datový formát pro výměnu GPS dat mezi programy a pro jejich sdílení mezi uživateli. Tento formát je podporovaný mnoha výrobci, ať už přístrojů (Garmin, Sony Ericsson,…) nebo jen programů (Google Earth, GPS-Tracks…).

V těchto souborech je velké množství různých dat, nás budou ale hlavně zajímat tyto tři, respektive dva, typy

- wpt (waypoint) - obsahuje individuální oblíbené uložené místo. Každé konkrétní místo je většinou specifikováno (liší se dle výrobce) zeměpisnou šířkou, zeměpisnou délkou, nadmořskou výškou, názvem místa, popisem místa, kategorií, ulicí, městem, obcí a PSČ.

```
<wpt lat="49.055790" lon="14.427638">
      <ele>-0.11</ele>
      <name>Domů</name>
      <desc>5. Května
      373 41 Hluboká Nad Vltavou, Č</desc>
      <extensions>
            <gpxx:WaypointExtension>
                  <gpxx:Address>
                        <gpxx:StreetAddress>5. Května </gpxx:StreetAddress>
                        <gpxx:City>Hluboká Nad Vltavou</gpxx:City>
                        <gpxx:State>České Budějovi</gpxx:State>
                        <gpxx:PostalCode>373 41</gpxx:PostalCode>
                  </gpxx:Address>
            </gpxx:WaypointExtension>
      </extensions>
</wpt>
```

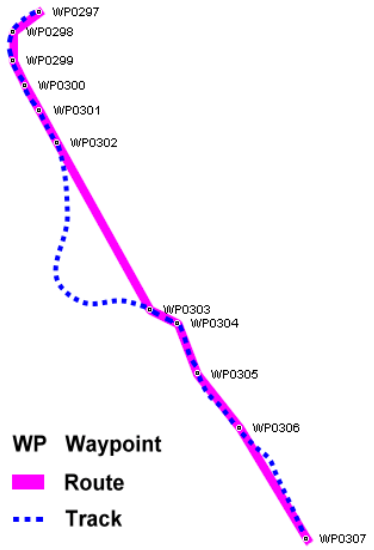
Obrázek 3 - uložené místo - GPX

- trk (track) - jsou to data, která jsou složena z alespoň jednoho segmentu, jež obsahuje body, které jsou logicky propojeny a ve výsledku tvoří trasu, kterou uživatel reálně projel. Každá *trk* je popsána jménem. Obsahuje segmenty, které na sebe navazují. Jeden segment skončí a druhý začne v případě ztracení signálu nebo v případě vypnutí přístroje. Segment je specifikován logicky propojenými body, jenž jsou určeny zeměpisnou šířkou, zeměpisnou délkou, nadmořskou výškou a časem v době vytvoření.

```
<trk>
    <name>Aktivní proto: 13 ZÁŘ 2015 11:45</name>
        <trkseg>
            <trkpt lat="49.159227" lon="16.626045">
                <ele>154.43</ele>
                <time>2015-09-13T09:45:16Z</time>
                <extensions>
                    <gpxtpx:TrackPointExtension>
                        <gpxtpx:speed>28.82</gpxtpx:speed>
                        <gpxtpx:course>87.53</gpxtpx:course>
                    </gpxtpx:TrackPointExtension>
                </extensions>
            </trkpt>
            <trkpt lat="49.159527" lon="16.633988">
                <ele>157.31</ele>
                <time>2015-09-13T09:45:36Z</time>
                    <extensions>
                        <gpxtpx:TrackPointExtension>
                            <gpxtpx:speed>30.20</gpxtpx:speed>
                            <gpxtpx:course>83.29</gpxtpx:course>
                        </gpxtpx:TrackPointExtension>
                    </extensions>
            </trkpt>
        </trkseg>
        <trkseg>
        ..
        </trkseg>
</trk>
```

Obrázek 4 - podniknutá cesta - GPX

- rte (route) - velice podobný formát dat jako *trk*. *Rte* také obsahuje logicky propojené body, které ve výsledku vytvoří trasu. Jediný rozdíl je v tom, že *rte* je cesta navrhovaná GPS přístrojem v době jízdy (potencionální trasa) a ne cesta, kterou uživatel skutečně projel. Většina navigací tyto data neukládá, ale pro kompletnost také uvádím.



Obrázek 5 – potencionální cesta - GPX

[https://en.wikipedia.org/wiki/GPS_Exchange_Format#/media/File:Wayroutrackp.png]

Pro získání informací ohledně přístroje (typ, verze map, ID apod.) se musíme v kořenovém adresáři dívat do souboru *Garmin/GarminDevice.xml*. Například, pro informace o konkrétním přístroji se v tomto souboru musíme podívat po řádce *<Device><Model><Description>XXX</Description></Model></Device>*. Pro získání dat týkajících se cestování musíme však hledat jinde. Uložená místa (typ dat *wpt*), ať už od uživatele nebo výrobce, musíme hledat v souboru *GPX/Current.gpx*. Trasy, které s Garmin navigací byli v minulosti projety, (typ dat *trk*) jsou uloženy na místě *GPS/Archive/x.gpx*, kde *x* je číslo konkrétního souboru. Množství zde uložených souborů se liší dle používanosti GPS. Nový *.gpx* soubor se vytvoří po dosažení 10 000 uložených bodů cesty.

3.2.2 TomTom

S navigací značky TomTom už je vše složitější. První generace navigací data s oblíbenými místy ukládá do zašifrovaného souboru *MapSettings.cfg*, ke kterému výrobce neodtajnil šifrovací klíč. Data tedy nelze přečíst. Informace týkající se projetých tras většina navigací této značky vůbec neukládá. Pokud se však trefíme na typ, který si tyto informace zapisuje, opět přijdeme na to, že jsou šifrovaná. Nejsou zde uloženy všechny projeté trasy, najdeme zde jen obecné informace ohledně poslední cesty navigace a detaily o plánovaných cestách. Pokud byl k přístroji připojen i telefon, v navigaci mohou být informace o MAC adresách připojených telefonů, volaná telefonní čísla, přijaté a odeslané sms zprávy. Navíc zde občas můžeme najít i souřadnice posledního místa, kde byla GPS zapnuta. Tento údaj se při zapnutí velice rychle přepíše, v případě nutnosti udělání bitové kopie tedy doporučuji GPS přístroj nejdříve dát do Faradayova obalu, nebo být na místě, kde máme jistotu, že není GPS signál. Nejčastěji jsou tyto data uloženy ve složce, která se jmenuje stejně, jako používaná mapa. Navigace, kterou jsem analyzoval, ukládala tyto data do složky *Central_Europe_950_6492*.

Druhé generace navigací této značky se zatím nedají analyzovat žádným veřejné známým způsobem. Navigace se po připojení k PC totiž už nechová jako „mass storage“, ale představí se jako síťová karta a dostat se k datům je během na velice dlouhou vzdálenost.

Z navigace TomTom se mi nepodařilo získat relevantní informace ohledně uložených oblíbených míst nebo projetých tras.

Soubory, které může GPS obsahovat a mohli by nás zajímat:

- *ttgo.bif* - obsahuje informace ohledně konkrétního přístroje (model, ID, jazyk, aktuální mapa, hlas)

```
[TomTomGo]
DeviceName=TomTom XXL IQ Routes Edition
DeviceVersionHW=ONE XXL IQ Routes
DeviceSerialNumber=RW2140C04212
DeviceUniqueID=AKVGL A2D4S
RamDiskVersion=20100419
BootLoaderVersion=55237
LinuxVersion=515773
ApplicationVersionVersionNumber=9053
ApplicationVersion=520930.2
UserLanguage=C˘es˘tina
UserName=
```

Obrázek 6 - ttgo.big - TomTom

- *CurrentLocation.dat* - obsahuje poslední pozici přístroje
- *Jméno_Mapy_a_Verze/MapSettings.cfg* - obsahuje informace o uložených oblíbených místech, itineráře a další použité adresy - zašifrované

Navíc může obsahovat následující soubory, pokud byl k navigaci připojen telefon:

- *Settings.dat* - obsahuje MAC adresy v minulosti připojených telefonů, jejich bezdrátové nastavení, nastavení a data poskytovatele - zašifrované
- *Contacts/Called.txt* - obsahuje telefonní čísla volaná z připojeného telefonu
- *Contacts/Callers.txt* - obsahuje telefonní čísla, která volala připojený telefon
- *Contacts/Contacts.txt* - obsahuje seznam kontaktů připojeného telefonu
- *Contacts/Inbox.txt* - obsahuje přijaté sms zprávy
- *Contacts/Outbox.txt* - obsahuje odeslané sms zprávy
- *SIMCARD/mobility.sim* – obsahuje údaje o připojené SIM kartě
- *itn/temporary.iti* – obsahuje údaje o naplánované cestě [6]

```
144778|490033|Nemanická|4|
144846|490052|Jižní|0|
```

Obrázek 7 - temporary.ini - TomTom

3.2.3 MIO

Čínské navigace Mio jsou v Evropě velmi rozšířené. Kvalitou zpracování si s ostatními značkami nemají co vyčítat a po softwarové stránce jsou na tom velice dobře. Jejich nespornou výhodou je doživotní bezplatná aktualizace map, na což zákazníci slyší.

Získat z této navigace data o cestách a oblíbených místech je velmi složitá záležitost. Informace ukládá v šifrované SQLite3 databázi a i přes velké úsilí jsem se k datům v čitelném formátu nedokázal dostat.

3.2.4 BLAUPUNKT

Navigace značky BLAUPUNKT je dražší, ale velmi kvalitní navigace Německé výroby. V České republice celkem neznámý výrobce, v okolních zemích však rozšířenější. Přístroje této značky svá data uchovávají na různých místech, velmi detailně, ve velké míře a v čitelném formátu v textovém souboru.

Oblíbená místa jsou uložena v */LUCCA/favorites.txt* a ve formátu znázorněném na obr. 9.

```
SRUBEC|-|11|2818|-|Srubec|-|-|-|-|-|14.54064|48.94822|-|-|14.54064|48.94822|
```

Obrázek 8 - favorites.txt - Blaupunkt

Nedávné cíle trasy najdeme v */LUCCA/recent.txt* ve formátu viz. obr. 10.

```
-|-|11|2818|-|Pluhuv Zdár|-|-|-|-|-|14.89346|49.22416|-|-|14.89346|49.22416|
-|-|11|2818|-|Jindrichuv Hradec|-|Ceská|-|-|-|15.01208|49.14912|-|-|15.01080|49.15150|
```

Obrázek 9 - recent.txt - Blaupunkt

Pokud by nás zajímala adresa místa DOMOV, musíme se podívat do */LUCCA/prefs.ini* a hledat řádek viz. obr. 11.

```
hometarget = -|-|11|2818|-|Srubec|-|-|-|-|-|14.54064|48.94822|-|-|14.54064|48.94822|
```

Obrázek 10 - prefs.ini - domov - Blaupunkt

Poslední cíl cesty je v tom samém místě, avšak v řádku viditelném na obr. 12.

```
lasttarget = -|-|11|2818|-|Ceské Budejovice|-|-|-|-|-|14.47494|48.97387|-|-|14.47494|48.97387|
```

Obrázek 11 - prefs.ini - poslední cíl - Blaupunkt

V souboru */LUCCA/SimTemp.gps* můžeme najít i detailnější popis jedné z cest ve formátu GPGGA, který zaznamenal pohyb vozidla každých pár metrů.

```
$GPGGA,000010,4856.868652,N,01432.5154,E,1,08,1.1,203.9,M,48.0,M,,*46
$GPVTG,116.8,T,116.8,M,0019.5,N,0036.0,K*46
$GPGGA,000011,4856.865723,N,01432.5233,E,1,08,1.1,203.9,M,48.0,M,,*4F
$GPVTG,116.8,T,116.8,M,0019.5,N,0036.0,K*46
```

Obrázek 12 - SimTemp.gps - Blaupunkt

Vysvětlení formátu: GPGGA,hh,llll.ll,a,yyyyy.yy,b,c,dd,e.e,f.f,M,h.h,M,j.j,kkkk

Tabulka 1 - GPGGA

GPGGA	hh	llll.ll	a	yyyyy.yy
začátek řádky	číslo řádku	zeměpisná šířka	sever (N) nebo jih (S)	zeměpisná výška
B	c	D	e.e	f.f
východ (E) nebo západ (W)	identifikátor GPS kvality	počet viditelných satelitů	horizontální ředění přesnosti	nadmořská výška
M	h.h	M	j.j	kkkk
jednotka (metry) v měření nadmořské výšky	výška geoidu nad elipsoidem WGS84	jednotka (metry) měření výšky geoidu	zlepšování přesnosti GPS (nevyužito)	checksum

K přepočtu zeměpisné šířky a výšky do používanějšího decimálního formátu, musíme hodnotu minut vydělit šedesáti. Pokud je tedy hodnota zeměpisné šířky 4856.868652N, musíme oddělit stupně a minuty (48 a 56.868652) a minuty poté vydělit (56.868652/60) a výsledná hodnota zeměpisné šířky je 48.947811N.

Řádek GPVTG je používán k zaznamenání rychlosti v několika různých jednotkách. Nás bude zajímat jen předposlední údaj „0036.0“, což je rychlost kilometrech za hodinu. [7]

3.2.5 GoClever

GoClever navigace jsou rozšířenou značkou v České republice z důvodu velmi nízkých pořizovacích cen. Navíc bývá prodávána s doživotní měsíční aktualizací map zdarma, co je jako bonus k nízké ceně výborná koupě v poměru výkon/cena. Data jsou ukládána v pěkně čitelném textovém formátu. Oblíbená místa se ukládají v *MobileNavigator/favs.txt* (obr. 14).

```
AREA="Jihozápad" CITY="Jankov (Holašovice)" COUNTRY="Česká Republika" POI="Špejchar u Vojty"
PT="14.273118 48.969999" TYPE="460" USED="1463829642" WPT="10642808 41996968"
PT="122.000017 24.999992" TYPE="-1" WPT="90969806 19262663"
```

Obrázek 13 - favs.txt - GoClever

V *MobileNavigator/recents.txt* jsou uloženy poslední cíle cest ve formátu viz. obr. 15.

```
AREA="Střední Čechy" CITY="Kolín" COUNTRY="Česká Republika" PLZ="28121"
POI="Kolín dílny" PT="15.233907 50.011683" TYPE="642" USED="1474107726" WPT="11359224 43192800"
AREA="Severovýchod" CITY="Jičín" COUNTRY="Česká Republika" PLZ="50601"
POI="Jičín" PT="15.360968 50.430447" TYPE="640" USED="1474091084" WPT="11453968 43680832"
```

Obrázek 14 - recents.txt - GoClever

4 NÁVRH PROGRAMU

4.1 POŽADAVKY

- program bude nainstalován na live distribuci
- data bude analyzovat z bitové kopie paměťového média GPS
- pokusí se získat veškerá data o trasách a oblíbených místech a umožní je zobrazit v GUI programu
- získané informace bude možné exportovat

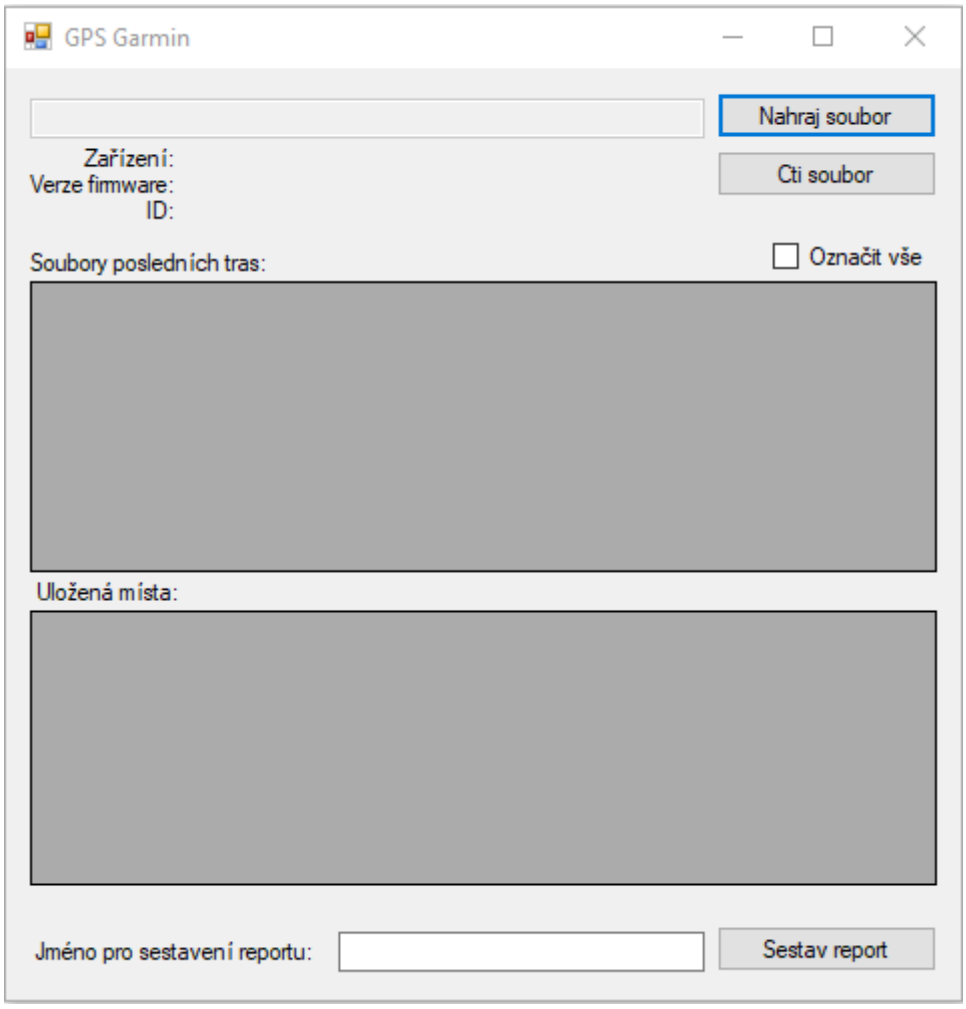
4.2 POUŽITÉ TECHNOLOGIE

Jako vývojové prostředí bylo použito Visual Studio na operačním systému Windows 10. Aplikace je napsána v programovacím jazyce .NET C# a za pomocí mono-project je upravena pro práci v operačních systémech Linux a Mac OS. Aplikace je vytvořena tak, aby se při minimálním úsilí dala upravit pro multiplatformní použití.

Jako operační systém pro live distribuci bylo plánováno použití bezpečnostní distribuce Deft. Ten však časem přestal být aktualizovaný a použitelný pro naše potřeby. Následnou distribucí byl zvolen penetrační Kali Linux, z kterého se mi však ve finálním kroku nepodařilo vyrobit live verzi. Díky jednoduchosti, svižnosti a lehké přenositelnosti se stalo další možností Ubuntu, které bylo nakonec zvoleno jako to pravé pro naše využití.

4.3 GRAFICKÉ PROSTŘEDÍ

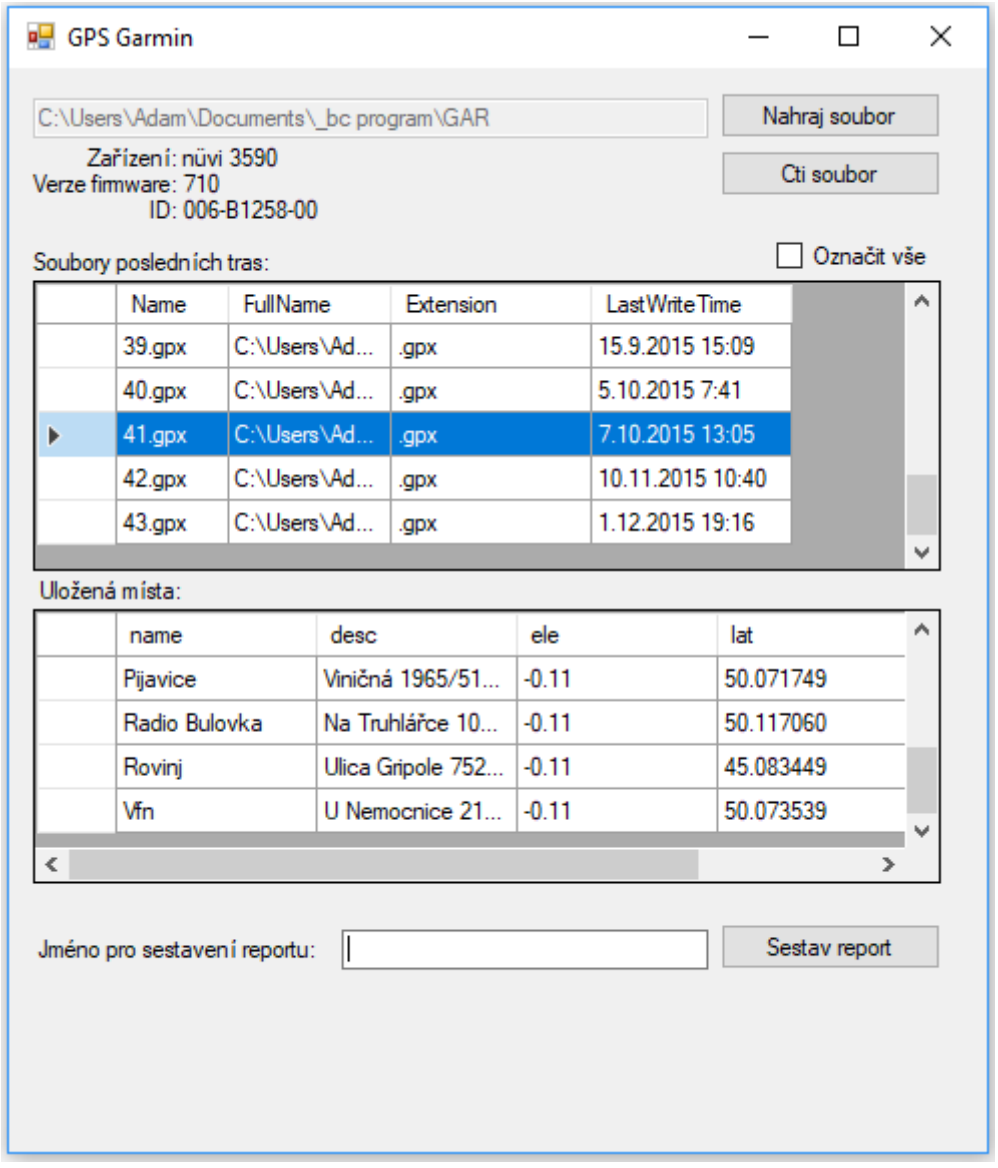
Prostředí je navrženo pro snadné, rychlé a intuitivní ovládání. Pevná velikost okna, statické rozvržení ovládacích prvků a uzpůsobení pro maximální efektivitu práce s aplikací.



Obrázek 15 - základní okno - program

Do první části patří vybrání cesty k bitové kopii. Tlačítko pro tento účel je umístěno v pravém horním rohu okna aplikace. Po stisku tlačítka „Nahraj soubor“ dojde k vyvolání souborového dialogu v novém okně, ve kterém uživatel vybere konkrétní bitovou kopii pro provedení analýzy. Aplikace je navržena tak, aby rozpoznala, o jaký model a výrobce GPS se jedná. Po výběru bitové kopie je uživateli umožněn stisk tlačítka „Čti soubor“ pro spuštění analýzy dat.

Aplikace se pokusí analýzou struktury dat zjistit, o který z nastudovaných modelů se jedná. Uživateli je zobrazena informace o úspěšném rozpoznání GPS. V opačném případě je zobrazeno chybové hlášení. Během načtení je automaticky vyplněna hlavička analýzy obsahující základní údaje o GPS (typ zařízení, verze FW a výrobní ID zařízení).



Obrázek 16 - zobrazení dat - program

Druhá část aplikace je určena pro zobrazení analyzovaných dat, jenž v sobě obsahují informace o trasách uložených v GPS. Například u navigací značky Garmin jsou vypsány všechny *.gpx* soubory. Při dvojkliku na jednotlivé záznamy jsou příslušná data zobrazena v open-source programu Viking, který je schopen vizualizace v uložených off-line mapách.

V panelu pod nápisem „Uložená místa:“ se zobrazují všechna oblíbená uložená místa, která GPS obsahovala. Jsou zde zobrazeny i detaily ohledně každého místa, konkrétně název bodu, jeho popis (do kterého je při nevyplnění uživatelem automaticky zapsána adresa bodu) následuje nadmořská výška, zeměpisná šířka a zeměpisná výška. Při dvojkliku na jakékoliv z uložených míst se opět zobrazí jeho umístění v programu Viking.

Třetí část se zaměřuje na vytvoření reportu. Podmínkou pro jeho vytvoření je zadání jména uživatele, které je následně zohledněno i v reportu. Pro zadání zde slouží pole s názvem „Jméno pro sestavení reportu:“. Výsledný dokument obsahuje všechna uložená místa a zvolené soubory posledních tras. Ty si můžeme vybrat za pomocí klávesy shift a kliknutím na jednotlivé trasy, nebo můžeme tlačítkem „Označ vše“ vybrat trasy všechny. Při zmáčknutí tlačítka „Sestav report“ je zobrazen dialog pro výběr umístění reportu.

5 PROGRAM

5.1 NAČTENÍ BITOVÉ KOPIE

Uživatelem vybraná bitová kopie GPS je připojena v OS Linux jako read-only, aby nedošlo k narušení integrity zkoumaných dat. Dialog pro výběr bitové kopie je vyvolán obsloužením události **Click** nad objektem **DataLoad** třídy **System.Windows.Forms.Button**. V momentě načtení je proveden pokus o připojení (mount) bitové kopie do systémové složky */mnt*. Pokud je toto propojení úspěšné, tak následně dojde k povolení objektu **DataRead** třídy **System.Windows.Forms.Button**. Obsluha události **Click** objektu **DataRead** se již následně stará o samotné parsování dat do připravených objektů třídy **System.Windows.Forms.DataGridView**. Rozpoznání prozkoumaných GPS je provedeno na základě analýzy souborové struktury a obsahu klíčových systémových souborů. Pokud tyto soubory nejsou přítomny, tak se může jednat o atypický či nenastudovaný model GPS nebo o poškozenou bitovou kopii.

5.1.1 GARMIN

Bitová kopie navigací Garmin obsahuje systémový soubor */Garmin/GarminDevice.xml*. Bylo zjištěno, že výrobce tento soubor a stejnou strukturu používá u většiny modelů.

5.1.2 BLAUPUNKT

Prozkoumané modely Blaupunkt obsahují systémový soubor */LUCCA/Device.bin*. U ostatních modelů této značky se dá předpokládat podobná organizace systémových souborů.

5.1.3 GOCLEVER

Analýza u výrobce GoClever je zaměřena na soubor */MobileNavigator/passport.txt*.

5.1.4 TOMTOM

Navigaci TomTom poznáme podle souboru *MapSettings.cfg*.

5.1.5 MIO

Navigaci Mio poznáme podle souboru *MioMap/MioMap/iGO.db*.

5.2 ANALÝZA

Po rozpoznání modelu a výrobce je uživatel informován vyskakovacím oknem. Program se zde větví z důvodu, že různé značky navigací používají odlišné umístění a strukturu dat. Samotná analýza je následně provedena funkcemi XXXXXLoad(), která je pro každého výrobce napsána zvlášť s ohledem na strukturu dat a souborů.

5.2.1 GARMIN

Analýza GPS Garmin je prováděna funkcí **GarminLoad()**. Základní údaje o modelu GPS jsou umístěny v souboru */Garmin/GarminDevice.xml*. Tento soubor je v podobě čistého XML a je tedy parsován do dočasného objektu **DataSetData** třídy **System.Data.DataSet** za využití metody **ReadXml**. Požadovaná data se zobrazí v prostředí aplikace pomocí vlastností **Text** objektů **DeviceName**, **DeviceFW** a **DeviceID** třídy **System.Windows.Forms.Label**.

Jelikož společnost Garmin používá standardní formu uložení záznamů v podobě *.gpx* souborů, bylo proto přistoupeno pouze k nalezení všech dostupných souborů a zobrazení jejich odkazem v objektech třídy **System.Windows.Forms.DataGridView**. Pro toto odkázání (nalezení souborů *.gpx*) byla použita metoda **GetFiles()** třídy **System.Data.DirectoryInfo**.

Data v poli „Uložená místa“ byla načítána stejným způsobem jako informace o GPS, jen ze souboru */GPX/Current.gpx*. Tento soubor je opět čisté XML a je tedy parsován do dočasného objektu **DataSetData** třídy **System.Data.DataSet** za využití metody **ReadXml**.

5.2.2 BLAUPUNKT

Analýza GPS Blaupunkt je prováděna funkcí **BlaupunktLoad()**. Základní údaje o přístroji jsou umístěny v souborech *LUCCA/Device.bin* a v */LUCCA/recent.txt*. Specifická struktura dat je zde parsována do třídy **System.Windows.Forms.DataGridView** pomocí metody **Split()** třídy **System.String**. Jako delimiter dat je použit znak „|“.

5.2.3 GOCLEVER

Analýza GPS GoClever je provedena pomocí funkce **GoCleverLoad()**. U zařízení této značky se výrobce pravděpodobně zaměřil na univerzálnost celé platformy. Není tak v systémových souborech obsaženo přímé označení modelu. Jediný čitelný identifikační údaj je tak sériové číslo zařízení v souboru */MobileNavigator/passport.txt*.

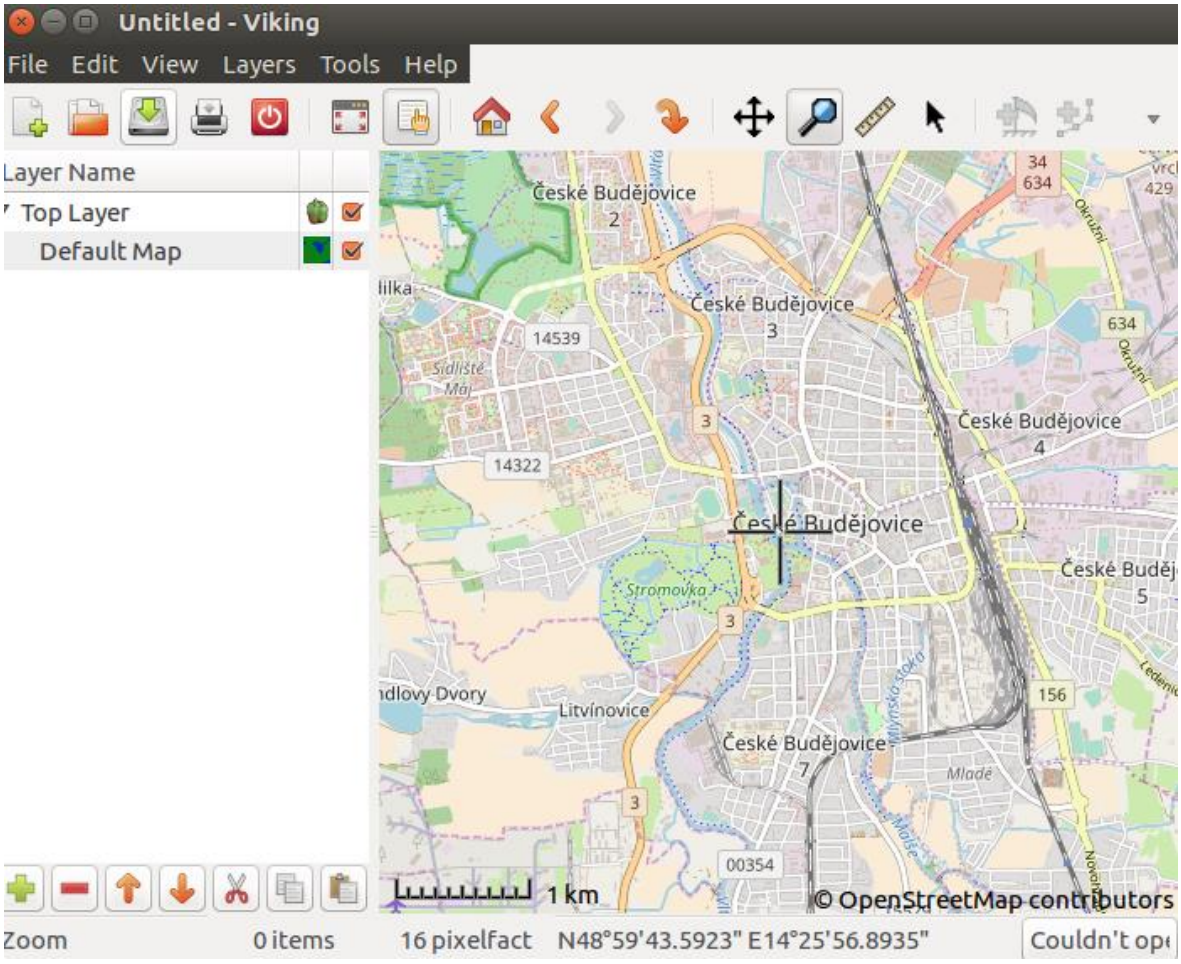
Stejně jako u zařízení Blaupunkt je zde struktura dat řešena na bázi řádkového zápisu v UTF-8. Zde je ovšem zápis zajímavě proveden pomocí neuspořádaných „tagů“, kde se k parsování používá regulárních výrazů s fixně danými prefixy. Parsování je tedy prováděno do objektů třídy **System.Windows.Forms.DataGridView**, pomocí metody **Match()** třídy **System.Text.RegularExpressions.Regex**.

5.2.4 TomTom & Mio

U těchto dvou výrobců je získání informací o pohybu nemožné, potřebné soubory jsou totiž zašifrované. Z tohoto důvodu se nedalo pokračovat v analýze TomTom a Mio GPS zařízení.

5.3 Vizualizace

Aplikace umožňuje zobrazit uložená oblíbená místa a projeté trasy na mapě v programu Viking. V závislosti na značce GPS je použito dvou způsobů zobrazení. U výrobců, kde se využívá standardní ukládání do *.gpx* souborů, jsou načítány přímo tyto soubory. V případech, kde je použito uložení v prostém textu, jsou parsováním načtená požadovaná data v podobě zeměpisné šířky a délky. Ty jsou poté programu Viking předloženy v podobě spouštěcích argumentů. Mapy, jenž program Viking používá, jsou staženy v offline podobě. Lze tak zajistit korektní zobrazení i bez přístupu k internetu.



Obrázek 17 - zobrazení dat na mapě – Viking . program

5.4 REPORT

Pro všechny navigace je vytváření reportu postaveno na stejném režimu. Z důvodu nutnosti zachování dat v nezměněném formátu bylo přistoupeno pro metodu přímého zrcadlení dat ze zdrojových souborů. Nemůže tak dojít k žádnému zkreslení oproti originálním datům.

Export dat do reportu je proveden pomocí metod třídy **System.IO.File**. Hlavní použitou metodou byla **AppendAllText()**, která nejen že umí provést zápis **string** proměnné s požadovaným kódováním, ale zároveň umí provést kopii textu přímo ze zdrojového souboru bez jakékoliv změny. Není tak ani omezena maximální délkou datových typů, což je obzvláště výhodné. Některé navigace totiž používají „nekonečných řádek“ pro ukládání dat. Standardní pomocný výstup reportu před dalším zpracováním je vždy proveden do běžného textového souboru formátu *.txt*. V tom souboru je zachované absolutně shodné formátování, jako má výrobce navigace v systémových souborech.

Druhou možností je vytvoření souboru ve formátu *.pdf*. Generování PDF je prováděno pomocí „virtuálního tisku“ na požadovaný formát papíru A4 pomocí rozšířených funkcí open-source balíčku *libreoffice* příkazem **soffice –convert-to pdf inputfile.txt**.

```
Report sestavil: test2
            Dne: 12/8/2017 12:19:06 PM
       Zařízení:GoClever
 Verze firmware:
             ID:
EUFJHwsAEAcBGQhbUEM8BgkiIUNCSQoKNRcOHRQICw9MUUdPRFFJQ0UbARMBNAwdSFtJW1ZUUFJaXl1KWlVTW19UIlJeW1VJWlB

Uložené body:
AREA="Jihozápad"CITY="Jankov (Holašovice)"COUNTRY="Česká Republika"PLZ=""POI="Špejchar u
Vojty"PT="14.273118 48.969999"RC=""STREET=""TYPE="460"USED="1463829642"WPT="10642808
41996968"WRC=""
AREA=""CITY=""COUNTRY=""PLZ=""POI=""PT="122.000017
24.999992"RC=""STREET=""TYPE="-1"USED=""WPT="90969806 19262663"WRC=""

Výpis vybraných (projetých tras):

Line: 28
AREA="Jihozápad"CITY="Jankov (Holašovice)"COUNTRY="Česká Republika"PLZ=""POI="Špejchar u
Vojty"PT="14.273118 48.969999"RC=""STREET=""TYPE="460"USED="1463829642"WPT="10642808
41996968"WRC=""

Line: 27
AREA="Moravskoslezsko"CITY="Ostrava (Moravská Ostrava)"COUNTRY="Česká
Republika"PLZ="70100"POI="Naučná stezka Slezská Ostrava - 12 - Sýkorův most"PT="18.296249
49.836778"RC=""STREET=""TYPE="400"USED="1463920297"WPT="13642672 42990224"WRC=""
```

Obrázek 18 - report - program

6 TEST APLIKACE

Program byl otestován na dvou různých navigacích od každé značky (Garmin, Blaupunkt, GoClever).

Tabulka 2 - test programu

	typ zařízení	verze FW	ID zařízení	podniknuté cesty	uložená místa	další
Garmin	X	X	X	X	X	
Blaupunkt		X	X	X*	X	
GoClever				X**	X	
TomTom						X***
Mio						

*jen poslední cesta **data jen o cílech cest ***data z telefonu

Dle tabulky výše je patrné, že program si dokázal poradit se všemi použitými navigacemi.

Program správně rozpoznal značky navigací a následné načtení obrazů disků proběhlo v pořádku a bez porušení integrity dat.

U navigací značky Garmin nebyl problém ani s analýzou důležitých informací o přístroji, tak ani s oblíbenými místy a uloženými cestami. Program vždy vše správně načetl, vypsal a i report dopadl tak, jak měl. Analýza dokázala najít i různé informace, které v navigaci zůstali po připojení telefonu přes bluetooth.

U navigací Blaupunkt se lehce lišila získaná data mezi prvním a druhým přístrojem. Oba přístroje obsahovali jen skromné informace o projetých trasách, konkrétně jsem se dozvěděl vždy jen detaily ohledně poslední cesty. Oblíbená místa, informace o firmwaru a ID přístroje byly dostupné dobře a program je přečetl správně. Naopak, název zařízení se v ani jedné z navigací nalézt nedal. Rozdíl, který se však objevil na druhé navigaci Blaupunkt, byly chybějící informace o připojeném telefonu, tím pádem nebylo možné zjistit volaná a přijatá čísla. Problém ale nebyl v programu, jen na druhé navigaci nikdy nebyla využita funkce připojení telefonu přes bluetooth.

Ani jedna z navigací GoClever neobsahuje informace o typu a ID zařízení, ani verzi firmwaru. Analýza obou navigací našla detaily o oblíbených místech, naopak data o podniknutých cestách byla velmi omezená. Jediné, co GPS ukládají, jsou informace o cílech cest, nikoliv však kudy a jakým způsobem se do toho cíle navigace dostala.

7 POUŽITÍ LIVE DISTRIBUCE LINUX

Jako operační systém pro live distribuci byl nakonec zvolen Ubuntu verze 16.04. Na distribuci byly nainstalovány všechny potřebné závislosti a pro implementaci .DLL knihoven a .NET frameworku byl použit mono-project, což je open-source knihovna přímo podporována společností Microsoft.

Po úspěšném nabootování z přiloženého DVD zvolíme možnost spuštění „live - boot the Live System“. Po načtení operačního systému se objeví žádost o vyplnění hesla k uživateli gps. Jako heslo se zadá „GPS“ a dojde k přihlášení.

Obrázek 19 - plocha - program

8 ZÁVĚR

V rámci této bakalářské práce byla vytvořena jednoduchá, jednoúčelová live distribuce Linuxu s předinstalovanou aplikací „GPS“. Úkolem programu je analyzovat bitové kopie pamětí GPS přijímačů, zjistit všechny informace, které by mohli být užitečné, od podniknutých cest až po telefonní čísla volajících. Výsledný report je možné uložit ve formátu *.txt* a *.pdf*.

Při hlubším zkoumání této problematiky jsem se dostal k zajímavým zjištěním. Skutečnost, jak moc se vize společností vyrábějících velice podobný výrobek liší, je překvapující. Zatímco Garmin se snaží mít svá zařízení lehce přístupná, data modifikovatelná a v běžném otevřeném formátu, tak například TomTom je přesným opakem. U starších navigací této značky se data o používání na GPS sice ukládala, ale v minimálním množství a i tak šifrovaně. U nových navigací už člověk k datům nemá přístup vůbec a zatím neexistuje veřejně známý způsob, jak se k ním dostat. Pro přidání vlastních oblíbených míst nebo plánovaných tras uživatel nemá jinou možnost, než použít aplikaci této společnosti. Ta má však k bezproblémovému fungování velice daleko. Pokud má uživatel větší množství vlastních bodů a aplikace nebude spolupracovat, uživatel nemá šanci, jak do zařízení svá uložená místa rychlým způsobem dostat.

Nedostupnost dat na určitých navigacích se při psaní této bakalářské práce stala nečekaným, avšak nepřekonatelným problémem. Nepodařilo se mi získat mnoho dat z navigací TomTom a Mio, většinou kvůli šifrování.

Některé aplikace třetích stran však skromná data z těchto navigací dostat dokáží. Jediný zdarma, se kterým jsem přišel do styku, je **PoiEdit**. Dokáže z TomTom navigace první generace vyčíst útržkovité informace o oblíbených místech. Není to však forenzní nástroj, ale povedený fanouškovský pomocník pro přidávání oblíbených míst do různých navigací a překlad z jednoho formátu do druhého. Druhým programem je **TomTology2**, který se soustředí pouze na TomTom a forenzním nástrojem je. Dle ohlasů funguje výborně, licence na rok však stojí 600 liber. Program, který jsem vytvořil, se ocitl někde uprostřed. Je forenzním nástrojem, nesoustředí se pouze na jednu značku navigací, nestojí žádné peníze. Na druhou stranu, určitě nemá takový rozhled jako PoiEdit a takovou kvalitu jako TomTology2.

Tím se nabízí dva nejvhodnější postupy, jak případně pokračovat v tomto směru i nadále. První cestou je pokračovat v analýze dalších GPS přístrojů a pokusit se vymyslet způsob, jak získat data i ze zašifrovaných jednotek. Dát programu lepší vzhled a optimalizovat výkon. Druhou cestou je tento pohled úplně opustit a vydat se směrem k stále se zvětšujícímu množství navigačních aplikací na mobilních zařízeních a jejich analýze…

Výsledná aplikace této bakalářské práce by měla díky zautomatizování forenzní analýzy GPS přístrojů zjednodušit a zkrátit potřebnou práci soudním znalcům a policii při zjišťování pohybu podezřelé osoby za pomocí dat z navigace.

Cíle práce byly částečně splněny.

CITOVANÁ LITERATURA

[1] ČÁBELKA, Miroslav. *Úvod do GPS* [online]. Praha, 2008 [cit. 2017-12-08]. Dostupné z: https://www.natur.cuni.cz/geografie/geoinformatika-kartografie/ke-stazeni/vyuka/gps/skriptum-uvod-do-gps?student_welcome=1. Skriptum. Karlova univerzita, Přírodovědecká fakulta, Katedra aplikované geoinformatiky a kartografie.

[2] Forenzní analýza. *RAC - Forenzní analýza* [online]. Praha: Risk Analysis Consultants [cit. 2017-12-09]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ZU-FA

[3] LIMBERG, Tomáš. *Forenzní vědy a jejich využití v kriminalistice* [online]. Brno, 2010 [cit. 2017-12-03]. Dostupné z: https://is.muni.cz/th/208268/pravf_b/Tomas_Limberg_-_208268_-_bakalarska_prace.pdf. Bakalářská práce. Masarykova univerzita, Právnická fakulta, Katedra ústavního práva a politologie. Vedoucí práce Pavel Kandalec.

[4] A Guide To The Global Positioning System (GPS). In: RadioShack [online]. Texas: RadioShack, 2005 [cit. 2017-12-11]. Dostupné z: https://web.archive.org/web/20100213100725/http://support.radioshack.com/support_tutorials/gps/gps_tmline.htm

[5] United States Updates Global Positioning System Technology. *America.gov* [online]. Washington, D.C.: Cheryl Pellerin, 2006 [cit. 2017-12-04]. Dostupné z: https://web.archive.org/web/20080305214526/http://www.america.gov/st/washfile-english/2006/February/20060203125928lcnirellep0.5061609.html

[6] 'Add to TomTom' Web Developers Guide. In: *TomTom* [online]. AC Amsterdam, The Netherlands: TomTom [cit. 2017-12-10]. Dostupné z: https://www.tomtom.com/lib/doc/TomTomTips/index.html?itinerary_as_text_file.htm

[7] GPS - NMEA sentence information. *GPS - NMEA sentence information* [online]. Nizozemsko: Glenn Baddeley, 2001 [cit. 2017-12-09]. Dostupné z: http://aprs.gids.nl/nmea/

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

PŘÍLOHA 1 - PROGRAMÁTORSKÁ DOKUMENTACE

Globální proměnné

int Manuf

- indexování výrobce navigace „Manufacturer“

bool ImageConnected

- stavová proměnná držící stav připojení bitové kopie

string ImageMD5

- přenos a uložení kontrolního součtu MD5

string XXXXXStart

- řada proměnných držící prefixy pro analýzu pomocí regulárních výrazů

string RegEnd

- proměnná drží postfix ukončující regulární výrazy

Objekty

System.Data.DataSet DataSetData

- objekt držící strukturu použitou jako zdroj dat pro zobrazení pomocí objektu **DataGridView**

System.Windows.Forms.TextBox Path

- objekt použitý primárně pro zobrazení systémové cesty k připojené bitové kopii

System.Windows.Forms.Textbox ReportName

- objekt použitý pro zadávání jména uživatele a pro sestavení reportu

System.Windows.Forms.Button DataLoad

- tlačítko zajišťující ověření existence, konzistence a správnosti bitové kopie
- tlačítko zároveň zajišťuje „mount“ samotné bitové kopie

System.Windows.Forms.Button DataRead

- tlačítko pro odstartování čtení dat navigace
- odděleno od **DataLoad** z důvodu, že multiplatformní prostředí mono není schopné zajistit dostatečný timeout nad systémovými vlákny

System.Windows.Forms.Button ReportThis

- tlačítko pro spuštění vytváření reportu

System.Windows.Forms.Label DeviceName

- popisek držící jméno zařízení (použití jako viditelná proměnná)

System.Windows.Forms.Label DeviceFW

- popisek držící verzi firmware zařízení (použití jako viditelná proměnná)

System.Windows.Forms.Label DeviceID

- popisek držící ID zařízení (použití jako viditelná proměnná)

System.Windows.Forms.Label label1, label2, label3

- variace popisek GUI

System.Windows.Forms.DataGridView dataGridView1, dataGridView2

- tabulkový zobrazovač pro vizualizaci dat načtených ze zařízení

Funkce pro čtení dat

Private void GarminLoad()

- obsluha a analýza dat navigace Garmin
- proměnné
    - **string PathVar**
        - drží cestu do přípojného bodu image navigace

Private void BlaupunktLoad()

- obsluha a analýza dat navigace Blaupunkt
- proměnné
    - **string PathVar**
        - drží cestu do přípojného bodu image navigace
    - **string Lines[], Fields[]**
        - list typu string použitý pro práci s víceřádkovým textem
    - **string CSVFilePathName**
        - proměnná cesty k souborům navigace a uložených pozic
    - **int Cols**
        - počet jednotlivých sloupců v souboru
- objekty
    - **System.Data.DataTable dt**
        - Dočasná datová tabulka pro parsování dat před importem do proměnné **DataSetData**

Private void GoCleverLoad()

- obsluha a analýza dat navigace GoClever
- proměnné
    - **string PathVar**
        - drží cestu do přípojného bodu image navigace
    - **string Lines[], Fields[]**
        - list typu string použitý pro práci s víceřádkovým textem
    - **string CSVFilePathName**
        - proměnná cesty k souborům navigace a uložených pozic

    - **int Cols**
        - počet jednotlivých sloupců v souboru
- objekty
    - **System.Data.DataTable dt**
        - Dočasná datová tabulka pro parsování dat před importem do proměnné **DataSetData**

Private string CalculateMD5 (string filename)

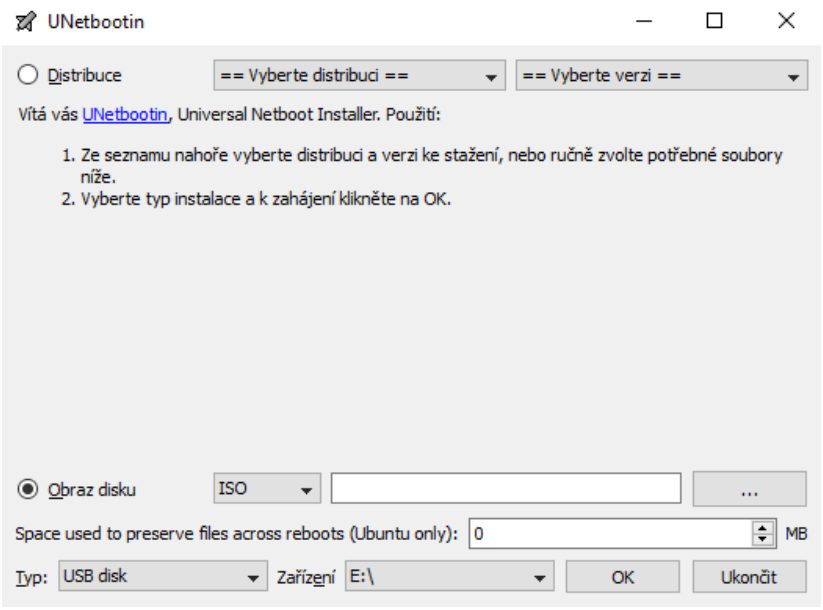
- výpočet kontrolních součtů vložených dat
- proměnné
    - **string Hash**
        - uložení vypočteného kontrolního součtu
- objekty
        - **System.Security.Cryptography.MD5 md5**
            - metody
                - **ComputerHash(string path)**
                    - výpočtení kontrolního součtu ze souboru

PŘÍLOHA 2 - UŽIVATELSKÁ PŘÍRUČKA

Vytvoření live distribuce

Pokud chceme vytvořit live distribuci na DVD, musíme soubor GPS.img vypálit na prázdné DVD.

Pokud je naším cílem live USB, vložíme prázdnou USB paměť do konektoru v počítači a vytvoříme live usb za pomocí programu (např. UNetbootin).



Obrázek 20 - UNetbootin

Spouštění live distribuce

Při použití CD nebo DVD počítač restartujeme a ujistíme se, že v BIOSu máme nastavené bootování z CD/DVD mechaniky. Při zapínání odsouhlasíme bootování z CD/DVD a následně vybereme možnost „live – boot the Live System“.

Při použití live usb je postup podobný. V BIOSu nastavíme bootování z USB disku. Při zapínání odsouhlasíme nabootování z USB a poté vybereme možnost „live – boot the Live System“.

Po načtení se operační systém zeptá na heslo, které je: „GPS“.

Spuštění programu GPSforensics

Program spustíme dvojklikem na ikonku GPSforensics.sh, která se nachází nahoře vlevo na ploše.

Práce s programem

Po startu programu máčkneme na tlačítko „Nahraj soubor“ a vybereme bitovou kopii navigace, kterou chceme analyzovat. Program kopii ihned načte a pokračujeme tlačítkem „Cti soubor“. Pokud se analýza dokončila v pořádku, zobrazí se získané titulní informace, soubory posledních tras a uložená místa. Pro zobrazení bodu nebo cesty na mapě stačí na vybraný soubor dvakrát poklikat. Pokud chceme vytvořit report jen z několika souborů, stačí je označit za pomocí shiftu. Pokud chceme vytvořit report kompletní, můžeme všechny soubory označit stejným způsobem, nebo stačí máčknout tlačítko „Označ vše“. Pokud chceme pokračovat vytvořením reportu, stačí vyplnit „Jméno pro sestavení reportu:“ a následně stisknout tlačítko „Sestav report“ a vybrat místo pro uložení reportu.

Nyní můžeme program ukončit nebo pokračovat načtením další bitové kopie.