Extração e análise de memória volátil em ambientes Android: uma abordagem voltada à reconstrução de trajetórias com base no protocolo NMEA 0183

João Paulo Claudino de Sousa[1], João José Costa Gondim[2]

[1]Seção de Perícias de Informática – Polícia Civil do Distrito Federal (PCDF)
Brasília, DF – Brasil

[2]Departamento de Ciência da Computação – Universidade de Brasília (UnB)
Brasília, DF – Brasil.

jpclaudino@gmail.com, joao.gondim@gmail.com

Abstract. *Android devices are widely used and can function as GPS receivers. Time and position information are very relevant in the investigative field, however, data stored in non-volatile media may be limited with regard to the reconstruction of trajectories. This paper proposes a method for recovering messages with GPS coordinates stored in RAM memory of Android mobile devices. Finally, it was analyzed the feasibility of reconstruction of trajectories based on the NMEA 0183 protocol messages retrieved from RAM memory.*

Resumo. *Dispositivos Android são amplamente utilizados e podem funcionar como receptores GPS. Informações de tempo e posicionamento possuem grande relevância no campo investigativo, todavia, os dados armazenados em mídia não-volátil podem ser limitados no que diz respeito à reconstrução de trajetórias. Este trabalho propõe um método de recuperação de mensagens com coordenadas GPS armazenadas na memória RAM de dispositivos móveis Android. Por fim, foi analisada a viabilidade da reconstrução de trajetórias de dispositivos móveis com base nas mensagens do protocolo NMEA 0183 recuperadas da memória RAM.*

1. Introdução

Sistemas Android possuem grande relevância para comunidade forense, sendo que nos últimos anos, diversos trabalhos sobre a aquisição e análise de dados provenientes tanto de memórias voláteis como não voláteis foram produzidos.

No campo investigativo, informações de posicionamento são importantes pois podem fornecer elementos para elucidação da autoria e do *modus operandi* de algum fato delituoso. Além disso, dados de tempo e velocidade também são providos por receptores GPS, podendo ter relevância na elucidação de crimes e acidentes de trânsito.

Este artigo propõe um método de recuperação de mensagens com coordenadas GPS armazenadas na memória RAM de dispositivos móveis Android, a fim de reconstruir o trajeto trilhado pelo dispositivo.

Nesta linha, as especificações da *National Marine Eletronics Association* (NMEA), em especial a NMEA 0183, têm importância fundamental na comunicação

dos receptores GPS com os diversos tipos de aparelhos, uma vez que provêm uma forma padronizada de transmissão dos dados de posicionamento.

O restante do artigo é organizado da seguinte forma: na seção 2 são apresentados trabalhos correlatos, tanto na área de aquisição de memória RAM, quanto na área de forense em dispositivos GPS; na seção 3 é mostrado o funcionamento da *engine* de localização (*GL engine*), sendo explicado como são geradas mensagens do protocolo NMEA e como estas mensagens podem ser recuperadas da memória RAM; na seção 4 são apresentados os testes realizados em diferentes ambientes, com múltiplos aparelhos, bem como os resultados obtidos a partir da análise de imagens (*dumps*) da memória volátil dos dispositivos. Por fim, trabalhos futuros e a conclusão são apresentados na seção 5.

2. Trabalhos correlatos

A recuperação de memória volátil em dispositivos Android vem sendo amplamente explorada nos últimos anos, dada a importância para o mundo forense das informações contidas neste tipo de memória. Em [Sylve, Case, Marziale e Richard 2012], foi produzida uma técnica que utiliza um módulo do *kernel* para extração de memória (conhecido como dmd ou LiME - *Linux Memory Extractor*). O módulo realizava a extração da memória percorrendo a estrutura *iomem_resource* do *kernel* e realizando a tradução de endereços. Entretanto, esta abordagem tem como empecilho a necessidade de compilação do módulo para cada versão específica de *kernel*.

Também existem outros trabalhos visando a aquisição de memória RAM, como em [Thing, Ng e Chang 2010], [Muller e Spreitzenbarth 2013] e [Stüttgen e Cohen 2014], porém, nesta pesquisa, optou-se por utilizar o módulo LiME para extração da memória volátil, visto que seu funcionamento, do ponto de vista forense, não causa grandes impactos na evidência. A documentação[1] do LiME detalha todo o processo de compilação do módulo *kernel*, levando em consideração a arquitetura ARM.

No que diz respeito à recuperação de informações de posicionamento em sistemas de navegação por satélite, há estudos principalmente associados a dispositivos das marcas Garmim, TomTom e Mappy, como pode ser visto em [Nutter 2008)], [Eijk e Roeloffs 2010], [Arbelet 2014] e [Lim, Lee, Park e Lee 2014]. Também foram desenvolvidos estudos relativos a recuperação de mensagens do protocolo NMEA, como pode ser observado em [Si e Aung 2011], bem como estudos relativos à precisão dos dados obtidos pelos mecanismos de GPS dos dispositivos móveis, como em [Guido, Gallelli, Saccomanno, Vitale, Rogano e Festa 2014] e [Spreitzenbarth, Schmitt e Freiling 2012].

Por fim, no que tange a análise de dados de GPS em dispositivos Android, em [Maus, Höfken e Schuba 2011] foi desenvolvido um trabalho onde coordenadas de GPS eram recuperadas de arquivos de log e bancos de dados de aplicações, todavia a análise de memória volátil não foi explorada.

Este trabalho possui como diferencial a abordagem voltada à reconstrução de trajetórias utilizando-se de dados de velocidade, geoposicionamento e tempo recuperados da memória volátil.

[1] https://github.com/504ensicsLabs/LiME - acessado em 07 jan. 2016

3. Sistemas de posicionamento global na plataforma Android

Para que sejam extraídas coordenadas GPS da memória volátil, primeiramente é necessário entender a arquitetura dos sistemas Android e como se dá a comunicação do chip receptor GPS com as diversas camadas do sistema. A seguir, são abordados o protocolo NMEA e sua relação com a reconstrução de trajetórias de dispositivos móveis.

3.1. Protocolo NMEA

O protocolo NMEA 0183 é o mecanismo de comunicação padrão entre os receptores GPS e os *drivers* dos dispositivos receptores na arquitetura Android. A ideia do protocolo, no que diz respeito a coordenadas de posicionamento, consiste em enviar uma linha de dados, codificada em ASCII, que pode conter informações de posição, velocidade, tempo, dentre outros elementos processados pelo receptor GPS. Cada mensagem é iniciada com o caractere "$" e terminada com o retorno de carro e a alimentação de linha (CR/LF). Além disso, as mensagens têm um prefixo de duas letras que define o tipo de dispositivo (chamado de *TALKER Identifier*), seguido de três letras que definem o conteúdo da mensagem. Para receptores de GPS o prefixo utilizado é o "GP" [*National Marine Electronics Association* 2002].

O formato da mensagem é simples, de forma que os dados contidos em uma linha são separados unicamente por vírgula (*comma-separated format*). Também há um campo, no fim de cada mensagem, para verificação de integridade dos dados (*checksum*) que é separado do restante da mensagem pelo caractere "*".

Há uma grande quantidade de tipos de mensagens NMEA, entretanto, no escopo desta pesquisa, cujo foco é a recuperação de coordenadas de posicionamento, de dados temporais e de velocidades, dois tipos de mensagens têm maior relevância: GPGGA e GPRMC. A Figura 1 mostra exemplos das referidas mensagens. Maiores informações sobre a estrutura das mensagens podem ser encontradas na especificação NMEA 0183.

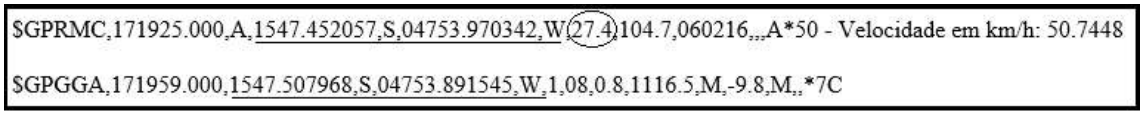

Figura 1. Mensagens GPRMC e GPGGA (coordenadas sublinhadas, velocidade, expressa em nós, circulada).

3.2. Arquitetura GPS em Sistemas Android

O sistema operacional Android possui o código fonte aberto (*open source*) o que facilita o entendimento de sua arquitetura. No que diz respeito à arquitetura GPS, o sistema pode ser dividido em camadas, que vão desde os aplicativos até o nível de hardware. Nas camadas mais acima estão os aplicativos e os *frameworks* que fazem uso de serviços de posicionamento.

Em nível de sistema, funcionando como base para os serviços de localização, existe toda uma *engine* para receber os dados do receptor GPS e fornecê-los para camadas superiores. A partir da versão 4.0 dos sistemas Android, alguns fabricantes começaram a utilizar o projeto GPSD para monitorar os receptores GPS embutidos nos aparelhos [GPSD Project 2015]. É importante ressaltar que alguns fabricantes não fazem

uso do projeto GPSD, possuindo outros mecanismos para gerenciar os dados de posicionamento. A *engine* também possui arquivos de configuração, geralmente em formato xml, que variam de nome e localização a depender da plataforma [*XDA Developers* 2012].

Nas camadas mais baixas existem os *drivers* e os chips receptores GPS. Os *drivers* utilizam API´s de baixo nível para se comunicar com o receptor GPS e geralmente consistem de um ou mais arquivos que se iniciam com o prefixo gps e terminam com a extensão ".so" [*XDA Developers* 2012].

4. Extração de Mensagens NMEA da memória volátil de sistemas Android

As mensagens NMEA perpassam praticamente todas as camadas da arquitetura GPS em ambientes Android, desde a comunicação *driver*/receptor até os *frameworks* em nível de aplicação. Como consequência, tais informações podem ser encontradas em diferentes regiões de memória, sendo de grande interesse forense, como é mostrado na seção 4.1. Na seção 4.2 é explicado o cenário de testes que foi montado para analisar a persistência dos dados na memória volátil, bem como quais técnicas podem ser utilizadas para preservar os dados.

4.1. Mensagens NMEA na memória RAM

As mensagens, como já dito anteriormente, são transmitidas por diversas camadas do sistema operacional. Por padrão, a especificação do protocolo NMEA estabelece que as mensagens são transmitidas em codificação ASCII. As camadas mais baixas da arquitetura GPS (*deamon gpsd* e os *drivers*) são escritas na linguagem de programação C, que geralmente trata *strings* como uma sequência de *bytes* codificados em ASCII. Desta forma, algumas mensagens serão encontradas na memória como uma simples sequência de caracteres codificada em ASCII, como pode ser visto na Figura 2.

Por outro lado, os aplicativos e *frameworks*, em ambientes Android, são escritos utilizando-se a linguagem de programação Java. Java é baseada no *charset* Unicode, o qual suporta a maioria dos símbolos utilizados no mundo. A especificação original do Unicode definia os caracteres como elementos de tamanho fixo, com 16 bits.

Entretanto, o padrão veio sendo alterado com o passar dos anos para permitir representações que necessitem de mais de 16 bits. Logo, as mensagens do protocolo NMEA, quando utilizadas nas camadas mais altas da arquitetura GPS, apresentam uma codificação diferente, utilizando mais *bytes*, como pode ser visto na Figura 2.

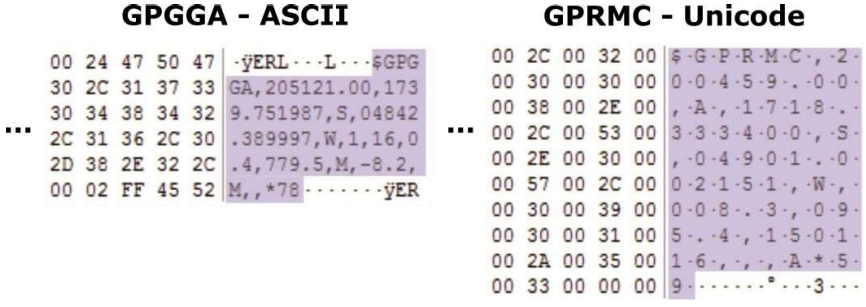

Figura 2. Mensagens GPGGA e GPRMC em ASCII e Unicode, respectivamente.

Para realizar a extração e análise dos dados, foi construída uma ferramenta que percorre o *dump* da memória RAM em busca de mensagens da especificação NMEA 0183, tendo como entrada um arquivo contendo a imagem da memória volátil e como saída arquivos de log e arquivos no formato GPX (*GPS Exchange Format*), que é um formato aberto para apresentação de dados de geoposicionamento. A ferramenta, que é de código aberto, está disponível no repositório Github[2].

4.2. Persistência das mensagens NMEA na memória volátil

O sistema operacional Android possui mecanismos diferenciados de gestão de memória que se adequam às especificidades dos dispositivos móveis. Consequentemente, a recuperação dos dados de posicionamento da memória volátil tem grande relação com o estado do sistema operacional no momento da coleta dos dados, ou seja, tem relação direta com o número de processos em execução, bem como a demanda por memória RAM por parte dos aplicativos nos momentos que antecedem a coleta dos dados.

Para melhor analisar a viabilidade da recuperação de dados de GPS em ambientes de reposta a incidentes, foram realizados testes em diferentes cenários com 4 dispositivos móveis. Os aparelhos escolhidos possuíam características diversas, utilizando diferentes versões do sistema Android e diferentes arquiteturas (ARM e x86). Os dispositivos utilizados podem ser visualizados na Tabela 1.

Tabela 1. Especificações dos dispositivos móveis

Fabricante/ Modelo	*Android*	Chipset	Memória
Samsung / GT-P5200 (*Tablet*)	4.2.2 (Jelly Bean)	Intel(R) Atom(TM) CPU Z2560 @ 1.60GHz	944372 kB
Samsung / SM-G3812B (*Smartphone*)	4.2.2 (Jelly Bean)	PXA1088 (ARMv7 Processor rev 3 (v7l))	804440 kB
Sony / LT22i (*Smartphone*)	4.1.2 (Jelly Bean)	NovaThor U8500 ARMv7 Processor rev 1 (v7l)	820588 kB
Sony / Z2 (*Smartphone*)	5.0.2 (Lollipop)	Qualcomm MSM8974PRO-AB (ARMv7 Processor rev 1 (v7l))	2846028 kB

Os experimentos foram realizados com o uso dos aplicativos Waze[3] e Google Maps[4], dada sua grande utilização pelos usuários Android. Os dispositivos foram inicialmente submetidos a *exploits* para escalada de privilégios e acesso como usuário administrador (*root*). Importante frisar que não foram utilizadas técnicas que envolvem substituição da partição *Recovery*, nem qualquer outra técnica que pudesse reiniciar o aparelho, visto que em casos reais o aparelho não pode ser desligado. Também foram previamente compilados módulos LiME para extração da memória RAM de acordo com as características de cada aparelho.

Para realização dos testes, todos os dispositivos foram colocados em modo avião, de forma a evitar o acesso a redes *wireless* e o acionamento do modo GPS assistido (A-GPS). Também foram removidos os cartões SIM (*simcards*). Desta forma, garantiu-se o uso dos aplicativos no modo *GPS only*. Para se obter os dados, foram realizados testes sob diferentes condições de tráfego e clima. Os dispositivos foram

[2] https://github.com/jpclaudino/nmeaSearch - acessado em 12 jun. 2016
[3] https://play.google.com/store/apps/details?id=com.waze - acessado em 17 jan. 2016
[4] https://play.google.com/store/apps/details?id=com.google.android.apps.maps - acessado em 17 jan. 2016

montados em um veículo de teste, que percorreu três rotas distintas. A primeira rota consistiu em um pequeno trecho de 4 km, a segunda em um trecho médio de aproximadamente 15 km e a terceira rota em um trecho longo de 150 km.

4.2.1 Experimento em rotas curtas

Os testes em rotas curtas consistiram em analisar o comportamento da memória RAM ao longo do tempo, verificando a viabilidade de reconstrução do caminho percorrido pelo dispositivo, mesmo já tendo passado um certo período de tempo. Foram realizados *dumps* da memória dos aparelhos durante um período de 30 minutos. Para cada dispositivo, após ser percorrido o trajeto de 4 km com um dos aplicativos ligados, o veículo foi parado e foi iniciada a recuperação dos dados da memória. A cada 5 minutos um novo *dump* de memória era produzido, com exceção do aparelho Sony Z2, que demandou 10 minutos, devido a maior quantidade de memória RAM.

Neste cenário, foram realizados dois tipos de testes. No primeiro, os serviços de localização do Android não foram interrompidos. Desta forma, os dados do receptor GPS continuaram sendo recebidos pelos aplicativos. No segundo caso, os serviços de localização foram desabilitados, no momento que o veículo parou, de forma que os aplicativos não mais conseguiam determinar rotas.

As imagens das memórias dos dispositivos foram então submetidas ao processamento pela ferramenta de extração e análise. A Tabela 2 mostra a quantidade de mensagens recuperadas de acordo com o tempo em que o *dump* foi realizado. O quadro quantitativo leva em consideração somente mensagens GPGGA e GPRMC válidas, ou seja, que continham coordenadas GPS.

Tabela 2. Quadro quantitativo de mensagens NMEA recuperadas a cada *dump*

Dispositivo	Serviço de Localização	Tempo transcorrido em minutos						
		0	5	10	15	20	25	30
Samsung GT-P5200	Habilitado	294	274	284	302	342	311	345
Samsung GT-P5200	Desabilitado	307	87	65	3	3	2	2
Samsung SM-G3812B	Habilitado	279	273	272	255	346	324	238
Samsung SM-G3812B	Desabilitado	86	46	26	24	22	12	8
Sony LT22i	Habilitado	275	364	355	382	396	431	316
Sony LT22i	Desabilitado	214	144	114	93	75	69	71
Sony Z2	Habilitado	1175	N/A	195	N/A	159	N/A	125
Sony Z2	Desabilitado	743	N/A	299	N/A	131	N/A	113

Observou-se que as coordenadas de posicionamento tendem a se agrupar no ponto de repouso do veículo, quando o serviço de localização estava ativo, como era de se esperar. Já a quantidade de mensagens recuperadas quando o serviço de localização estava inativo tende a reduzir com o passar do tempo, entretanto, em alguns dispositivos, as coordenadas de posicionamento recuperadas forneceram mais informações sobre o percurso completo, mesmo depois de transcorridos 30 minutos, se comparadas com aquelas recuperadas nos testes com o serviço de localização habilitado.

A Figura 3 mostra imagens, criadas com o software *Google Earth*[5], das coordenadas GPS recuperadas do dispositivo Sony Z2, nos testes realizados. É possível observar, na figura, que as coordenadas ao longo do trajeto foram perdidas depois de transcorridos 30 minutos, no cenário com os serviços de localização habilitados. Entretanto, no cenário com os serviços de localização desabilitados, foi possível reconstruir parcialmente a trajetória do veículo, mesmo depois de transcorridos 30 minutos.

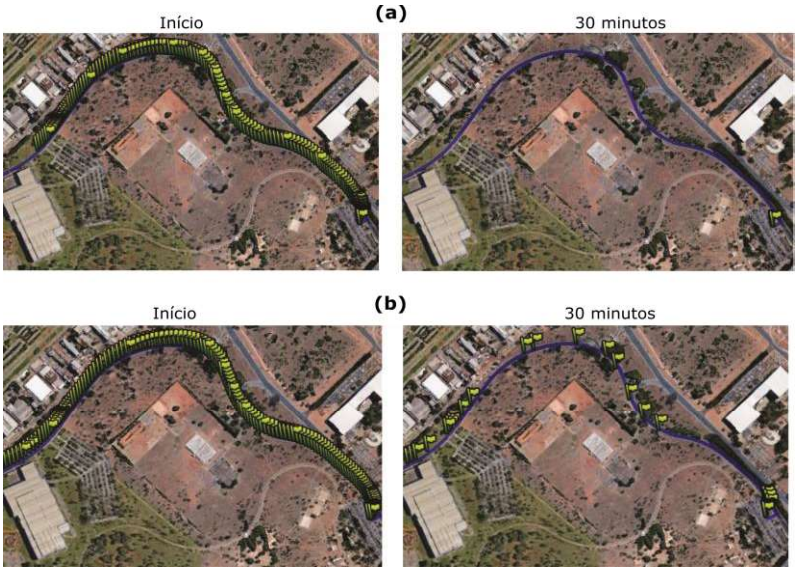

Figura 3. Coordenadas de posicionamento recuperadas do aparelho Sony Z2 nos testes com os serviços de localização habilitados (a) e desabilitados (b).

Os dados também mostram um comportamento diferenciado do aparelho Sony Z2, com uma alta taxa de mensagens recuperadas nos primeiros *dumps*, seguido de uma queda abrupta com o passar do tempo. Tal variação ocorreu devido ao fato de o aparelho em análise possuir a versão *Lollipop* do Android, que utiliza o *Android Runtime* (ART) como ambiente de execução, ao invés de seu predecessor *Dalvik*[6]. O sistema de gerenciamento de memória do ART foi aprimorado, principalmente no que diz respeito a *garbage collection*, sendo mais eficiente na liberação de memória.

Cabe ressaltar que, independentemente da abordagem utilizada (desligando ou não os serviços de localização), foi possível recuperar informações sobre determinados pontos do trajeto percorrido, inclusive com dados sobre velocidade e tempo.

4.2.2 Experimento em rotas médias

Para simular casos de condutores de veículos em ambientes urbanos, foi percorrido um trajeto de 15 km. Os dispositivos Samsung SM-G3812B e Sony Z2 foram testados em condições de clima desfavoráveis para o uso de GPS, com chuva intensa e nuvens carregadas. Assim como no caso anterior, o veículo foi parado e foi iniciada a recuperação dos dados da memória. Foram realizados *dumps* da memória dos aparelhos no período de uma hora. Nos primeiros 30 minutos, uma imagem era produzida a cada dez minutos. Depois deste período, foi feito um último *dump* depois de passados 60 minutos do veículo em repouso.

[5] https://www.google.com/earth - acessado em 02 jan. 2016
[6] https://source.android.com/devices/tech/dalvik - acessado em 07 jan. 2016

Neste cenário os serviços de localização não foram desligados, simulando casos de acidentes de trânsito, onde o tempo de reposta das equipes periciais geralmente é longo. A Tabela 3 mostra a quantidade de mensagens recuperadas ao longo do tempo. A Figura 4 mostra imagens das coordenadas GPS recuperadas do dispositivo Samsung GT-P5200, após transcorridos 60 minutos da primeira extração de dados. Importante observar que, mesmo transcorrido o intervalo de 60 minutos após o veículo entrar em repouso, foi possível recuperar informações do trajeto percorrido, bem como dados de velocidade, que podem ser muito importantes em investigações de acidentes de trânsito.

Tabela 3. Quadro quantitativo de mensagens recuperadas a cada *dump* (15 km)

Dispositivo	Tempo transcorrido em minutos				
	0	10	20	30	60
Samsung GT-P5200	177	243	337	315	330
Samsung SM-G3812B	11	293	336	303	377
Sony LT22i	200	363	177	333	272
Sony Z2	294	985	234	180	228

Os experimentos também mostraram que a precisão dos receptores GPS em condições climáticas adversas, como no caso de chuva intensa, pode ser altamente afetada. Os dados coletados do aparelho Samsung SM-G3812B mostram erros no cálculo de posicionamento que variaram entre 1200 m a 1500 m do percurso original, como pode ser visualizado na Figura 5. Neste sentido, deve-se levar em consideração outros aspectos das mensagens NMEA, as quais possuem informações sobre o número de satélites visíveis, bem como a precisão dos dados recebidos.

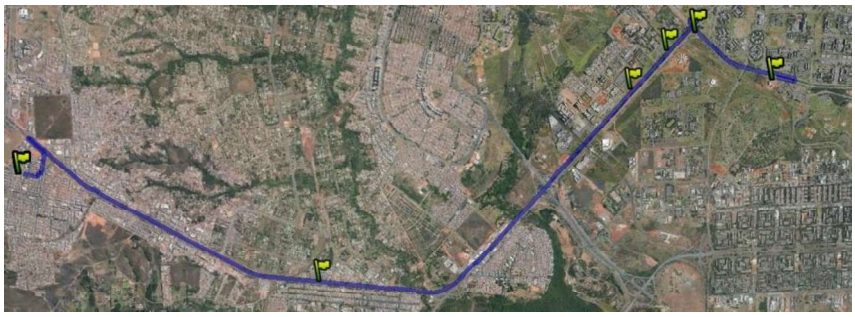

Figura 4. Plotagem dos dados recuperados do dispositivo Samsung GT-P5200, após transcorridos 60 minutos.

Figura 5. Erro de medição em condições climáticas adversas.

4.2.3 Experimento em rotas longas

Neste experimento, foi utilizado somente o Tablet Samsung GT-P5200. Foi percorrido um trajeto de 150 km em aproximadamente 2h. Ao final do trajeto, após 10 minutos com o veículo em repouso, foi realizado o processo de *dump* da memória RAM. Os dados foram então extraídos e analisados, tendo sido encontradas 392 mensagens NMEA na memória. Neste cenário, os dados foram coletados após uso contínuo e por um longo período do aplicativo Google Maps. Mesmo após o decurso de duas horas, foi possível recuperar informações de grande parte do trajeto, como mostrado na Figura 6.

Figura 6. Plotagem dos dados recuperados do dispositivo Samsung GT-P5200, após ser percorrido um trajeto de 150 Km.

O aplicativo fez uso de mais memória RAM do que nos testes anteriores, e mais dados persistiram por mais tempo. Algumas informações podem ter grande relevância forense e podem indicar o comportamento do usuário do dispositivo. Os dados recuperados, ainda que não forneçam precisamente todo o trajeto percorrido, contêm informações que permitem inferir aspectos como clima, tempo e velocidade média em determinados trechos.

5. Conclusão e Trabalhos Futuros

Neste artigo foi demonstrada a viabilidade da reconstrução de trajetórias de dispositivos móveis Android com base em coordenadas de posicionamento recuperadas da memória RAM. Além disso, foi feita uma análise da arquitetura GPS em sistemas Android, o que resultou na produção de uma ferramenta para recuperação de dados do protocolo NMEA 0183 relevantes no contexto forense.

Foi possível observar que diversos fatores podem ter influência na recuperação dos dados da memória RAM, como o estado do sistema operacional, a ferramenta de extração de dados e as configurações de software e hardware do dispositivo.

Desta forma, este trabalho se diferencia dos citados anteriormente uma vez que, além dos estudos na área de extração de memória volátil e forense em GPS, o estudo aborda a reconstrução da trajetória de dispositivos móveis com base no protocolo NMEA 0183.

Futuramente será construída uma ferramenta para analisar não somente as mensagens NMEA recuperadas da memória RAM, mas também outros dados com informações de GPS armazenadas no contexto das aplicações. Um dos grandes empecilhos para extração de dados da memória volátil é o procedimento utilizado atualmente, com o uso do módulo LiME, que depende da prévia compilação com base no *kernel* do dispositivo em evidência.

Trabalhos futuros podem explorar mecanismos de extração de memória RAM que independam de prévia compilação de *kernel*. Além disso, os dispositivos estão em constante evolução e periodicamente são lançadas correções de segurança que inibem a escalada de privilégios, o que demanda estudos constantes dos mecanismos de *rooting*.

Referências

Arbelet, A. (2014). Garmin satnav forensic methods and artefacts: an exploratory study. Doctoral dissertation, Edinburgh Napier University.

GPSD Project. (2015). gpsd - a GPS service daemon. Acessado em: 14 jan. 2016. http://www.catb.org/gpsd/index.html.

Guido, G., Gallelli, V., Saccomanno, F., Vitale, A., Rogano, D. and Festa, D. (2014). "Treating uncertainty in the estimation of speed from smartphone traffic probes." Transportation Research Part C: Emerging Technologies, 47, p. 100-112.

Lim, K. S., Lee, C., Park, J. H., and Lee, S. J. (2014). "Test-driven forensic analysis of satellite automotive navigation systems", Journal of Intelligent Manufacturing, 25(2), p. 329-338.

Maus, S., Höfken, H. and Schuba, M. (2011). "Forensic analysis of geodata in android smartphones.", International Conference on Cybercrime, Security and Digital Forensics, http://www. schuba. fh-aachen. de/papers/11-cyberforensics.pdf.

Müller, T. and Spreitzenbarth, M. (2013). "Frost", Applied Cryptography and Network Security. p. 373-388. Springer Berlin Heidelberg.

National Marine Electronics Association. (2002). NMEA 0183 - Standard for interfacing marine electronic devices, Version: 3.01. NMEA.

Nutter, B. (2008). "Pinpointing TomTom location records: A forensic analysis.", Digital Investigation, 5(1), p. 10-18.

Si, H. and Aung, Z. M. (2011). "Position data acquisition from NMEA protocol of global positioning system.", International Journal of Computer and Electrical Engineering, 3(3), p. 353.

Spreitzenbarth, M., Schmitt, S. and Freiling, F. (2012). "Comparing Sources of Location data From Android Smartphones.", Advances in Digital Forensics VIII. p. 143-157. Springer Berlin Heidelberg.

Stüttgen, J. and Cohen, M. (2014). "Robust Linux memory acquisition with minimal target impact", Digital Investigation, 11, S112-S119.

Sylve, J., Case, A., Marziale, L. and Richard, G. G. (2012). "Acquisition and analysis of volatile memory from android devices", Digital Investigation, 8(3), p. 175-184.

Thing, V. L., Ng, K. Y. and Chang, E. C. (2010). "Live memory forensics of mobile phones", Digital Investigation, 7, S74-S82.

Van Eijk, O. and Roeloffs, M. (2010). "Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems.", Digital Investigation, 6(3), p. 179-188.

XDA Developers. (2012). Understanding Android GPS Architecture. (n.d.). Acessado em: 14 jan. 2016. http://forum.xda-developers.com/showthread.php?t=2063295.

