PERÍCIA DIGITAL EM DISPOSITIVOS MÓVEIS

Michel Gargel NUNES, Fábio Eder CARDOSO
gargelmichel@gmail.com, fabioeder.professor@gmail.com

RESUMO: A área da tecnologia trouxe enormes vantagens para os negócios e para as pessoas, ajudando na mobilidade e nos processos de trabalho. Com esta explosão no uso de *smartphones*, todo mundo quer ter um ambiente *mobile*, fazendo uso de redes sem fio, acessando seus dados, e, carregando consigo informações privadas tanto corporativas, ou seja, referentes ao seu meio de trabalho, quanto, pessoais, como por exemplo, contato de amigos, familiares, fotos, etc. Entretanto, atrelado ao seu uso extremo, tornou-se notória a quantidade de crimes que tem ocorrido por meio do acesso vedado destes dados aos criminosos. Para este fim, os peritos corroboram esforços em prol da resolução destes crimes por meio da captura e análise de evidências, que, fazem parte do processo de investigação de referidos delitos em dispositivos móveis. Para auxiliar na investigação é que tem sido desenvolvidas as técnicas forense, que se dão por meio de ferramentas *software* e *hardware*, auxiliando nessa captura de evidências a serem analisadas pelo perito. Sendo assim, este trabalho busca apresentar, panoramicamente, uma distribuição Linux que se chama *Santoku*, como possibilidade de auxílio à perícia digital.

PALAVRAS-CHAVE: Perícia digital; computação forense; software; distribuição Linux; *AFLogical*.

ABSTRACT: The area of technology has brought huge benefits to business and people, helping mobility and work processes. With this explosion in the use of smartphones, everyone wants to have a mobile environment, making use of wireless networks, accessing their data, and carrying with them private information, both corporate, that is, referring to their work environment, such as contact with friends, family, photos, etc. However, coupled with its extreme use, the number of crimes that have occurred through the access of these data to criminals has become evident. To this end, the experts support efforts to solve these crimes by capturing and analyzing evidence, which is part of the investigation process of these crimes on mobile devices. To aid in the investigation is that forensic techniques have been developed, which are given through software and hardware

tools, helping in this capture of evidence to be analyzed by the expert. Thus, this work seeks to present, panoramic, a Linux distribution that is called Santoku, as a possibility of aid to digital expertise.

KEYWORDS: Digital expertise; forensic computing; software; Linux distribution; AFLogical.

1. Introdução

Este trabalho está dividido em três partes, e, busca apresentar como se deu o desenvolvimento das técnicas forenses no decorrer dos tempos com o intuito de reafirmar a sua importância para a sociedade atual. Inicialmente, tratar-se-á sobre a origem e evolução da mesma a partir da Idade Antiga, apresentando seus métodos iniciais, bem como, as ferramentas forenses. Posteriormente, será apresentado um esboço sobre os crimes cibernéticos, e, como eles tem influenciado do desenvolvimento e agregação das ferramentas *hardware* e *software* dentro da perícia forense. Por fim, mostrar-se-á na sessão "Ferramentas de *Software"* um possível método de perícia que captura de dados.

Por meio da tecnologia da informação, e da inserção massiva de dispositivos móveis no cotidiano das pessoas, muitos dos processos de trabalho tem sido afetados negativamente por conta dos crimes virtuais. Isso seria dizer que, os crimes virtuais superam os crimes mais comuns, como, furtos, roubos e até mesmo, assassinatos, sendo que seu principal veículo de atuação tem sido os aparelhos de smartphones.

Sabendo disso, tais crimes raramente são solucionados, quer pela ineficácia da polícia no tocante ao levantamento de provas, quer pelo criminoso, que, por meio de técnicas especiais não deixa vestígios do crime cometido. Assim as tecnologias acabam auxiliando os departamentos de segurança pública na solução ou no direcionamento de evidências para que tais ações criminosas sejam minimizadas.

A perícia digital é uma das técnicas de segurança que surgiu como uma possibilidade de solução, ou seja, para a redução de riscos de ocorrência de *cibercrimes*, ações que consistem em fraudar a segurança de sistemas computacionais (ALBUQUERQUE, 2006).

Segundo Eleutério e Machado (2011) a Perícia Forense ou Análise Digital Forense corresponde a modalidade de perícia criada para combater os crimes digitais por meio de análises e métodos que buscam a coleta e a identificação de evidências comprovadas. De acordo com (FREITAS, 2006) a forense computacional pertence ao ramo da

criminalística, assim, compreende a aquisição, prevenção, restauração e análise de evidências computacionais, sejam elas por componentes físicos, ou, por dados que foram processados eletronicamente e armazenados em mídias computacionais.

A distinção entre os crimes tradicionais e os crimes virtuais está no modo de operação, visto que, crimes virtuais utilizam de dispositivos eletrônicos (computadores, redes e da Internet) para a ação ou omissão do crime. Contudo, a tarefa de identificação, julgamento e penalização, se torna cada vez mais complexa devido à possibilidade de anonimato dos contraventores, e, ao fato de que as evidências do crime distribuírem-se em diversos servidores espalhados pela internet, tornando a prática de perícia forense computacional cada vez mais desafiadora.

2. Origem da perícia

Antigamente, quando o homem vivia em aglomerações tribais, a violência era identificada como uma ameaça ao grupo e significava uma quebra da confiança que deveria existir entre seus membros. A ameaça impedia a tribo de prosperar; a quebra de confiança colocava em risco a segurança de todos. Mediante a identificação e isolamento do indivíduo, a tribo, interrogava o criminoso exigindo uma justificativa, assim, após analisar a resposta, julgariam se o seu ato seria tolerado ou não.

A prisão do criminoso, por dada sociedade, dependia das provas de que o mesmo cometeu o crime, e, essas provas eram baseadas em relatos de outros membros que constituíam determinado grupo social. Entretanto, a declaração de um único indivíduo, bem como, os interesses escusos envolvidos, poderiam suscitar dúvidas quanto a veracidade do relato (RUIZ, 2005). Desse modo, perceberam que era necessário alicerçar esses relatos com evidências físicas, que pudessem elucidar o ato criminoso.

A insuficiente estrutura judiciária da tribo asseverou a importância da prova material, da necessidade de se fazer um exame de corpo de delito, e, assim surgiram as grandes perguntas forenses: Se alguém foi assassinado, onde estaria seu corpo? Se o agressor infligiu ferimentos à vítima, quais seriam esses? Se um objeto foi furtado, por que teria sido acusado este indivíduo? (RUIZ, 2005)

No período entre os séculos XVI ao XVIII, começaram a desenvolver a maior parte dos métodos e instrumentos forenses. Muitos progressos científicos apareceram e foram agregados ao arsenal utilizado para esclarecer crimes. Exemplificando tal dado histórico, temos que, o final do século XVI a invenção do microscópio, por Zacharias Jansen serviu para o esclarecimento de alguns tipos de vestígios.

Em meados de 1664, um médico italiano chamado *Marcelo Malphigi*, publicou um trabalho, cujo, o título era "Epístola sobre o órgão do tato", que apresentava um estudo sobre o desenho digital e palmar, sendo a remota origem da *papiloscopia*. No final do século XVIII, as armas começaram a ser produzidas com almas raiadas, e no século XIX, devido a isso, Henry Godard conseguiu relacionar uma bala com a arma utilizada. (LUQUE, 2002)

Outra grande invenção que contribuiu para a forense foi a fotografia, criada em 1826 e muito utilizada desde sua invenção. Thomas Byrnes, um detetive norte-americano, em 1886, publicou uma coletânea de fotos de criminosos, com o intuito de facilitar o reconhecimento de possíveis suspeitos. Tal prática vem sendo adotada até os dias de hoje. (GONZÁLEZ, 2004)

Anos antes, em 1815, Mathieu Orfila publicou um livro denominado *Traité des Poisons*, onde fazia uma classificação dos venenos que eram mais utilizados por criminosos. Orfila tornou-se o pai da Toxicologia, e, nessa mesma linha, James Marsh, um químico inglês desenvolveu a técnica para detectar vestígios de arsênico, por volta do ano de 1840.

Ainda que alguns dos métodos e ferramentas surgidos nessa época tenham ficado esquecidos, os conceitos estabelecidos serviram como base para diversas áreas da Ciência Forense, como a Balística e a Toxicologia. (LUQUE, 2002)

Sendo assim, a prática forense em dispositivos móveis, integra a grande categoria da forense digital, extraindo, recuperando e analisando as evidências digitais, ou, os dados de um dispositivo móvel, sobre condições forenses específicas.

Resumidamente, a perícia digital trata-se do acesso de dados armazenados em dispositivos, o que inclui SMS, contatos, registros de chamadas, fotos, vídeos, documentos, arquivos de aplicativos, históricos de navegadores, entre outros, e também trabalha na recuperação de dados deletados dos dispositivos, usando algumas técnicas forenses.

3. Crimes digitais

Há tempos o ser humano convive com os crimes e com a violência desde os primórdios da sociedade, entretanto, a mesma evoluiu, com isso, também os crimes e a violência, mas, em prol da manutenção da ordem, foram estabelecidas leis pelas autoridades. Dessa forma, a evolução da sociedade foi acompanhada pelo avanço tecnológico, que cada vez mais atinge as diferentes camadas da sociedade.

Os crimes crescem a cada dia, mas, para que um indivíduo seja condenado, é preciso que todo o processo seja cumprido. Parte desse rito é a materialização do crime cometido, feita tanto através da criminalística, quando da realização dos exames periciais. De acordo com Zarzuela (1996), para a criminalística, o delito, quando visto como um ato humano, deve ser apontado e comprovado de forma científica ou técnica, ignorando as causas, circunstâncias ou peculiaridades que levaram o indivíduo à sua prática. Este é o papel da Perícia Forense, seu objetivo é demonstrar, através de métodos científicos, a verdade, bem como, auxiliar na tomada de decisão final nos casos judiciais.

A perícia forense é utilizada em grande parte dos casos, porém, com métodos e exigências distintas para cada tipo de crime investigado. Com a crescente evolução das tecnologias na área computacional, a PFC tem se dificultado cada vez mais, porque, existem alguns paradigmas que na maioria das vezes tornam a análise e o levantamento de evidências menos ágil do que poderiam ser. É útil destacar que, a utilização de técnicas e ferramentas que dificultam a prática delituosa e seu autor, torna-se cada vez maior, o que faz o desenvolvimento de novos métodos e a busca por evidências digitais mais necessária.

Segundo Zillo Neto (2008), todos os dias novas tecnologias surgem e dela, a necessidade de novas preocupações com a segurança, novas especificações, novos padrões, e antes mesmo de implementar novas tecnologias seguras, aparecem outras, depois outras, e assim sucessivamente, virando uma corrida contra o tempo [...] Assim, a PFC zela pelo colhimento e guarda das provas de forma a evitar alterações e quebra de integridade das mesmas, isso seria dizer que, as provas analisadas devem permanecer da forma que foram encontradas (SHINDER, 2002). Entretanto, inúmeras provas surgem como ameaças digitais, e cada vez mais se utilizam de mecanismos de criptografia, que só podem ser analisadas quando estão em execução ou com o equipamento ligado, o que as leva a sofrer pequenas “alterações” (SECURITYFOCUS, 2007).

Em outras áreas da perícia, como a criminal, onde, se o método utilizado for cientificamente comprovado e reconhecido, a prova é "alterada" sem questionamentos. No processo pericial de uma arma de fogo, por exemplo, deve ocorrer o disparo com a arma em ambiente de laboratório para que seja feita a análise da prova do possível crime, mediante o disparo da arma, porque com ele ocorre uma “alteração” de provas. Isso não diz que a prova seja modificada a ponto de tornar-se inadmissível a perícia, porém, a mesma precisa ser manuseada e preparada para a análise.

Segundo (FREITAS, 2007), distintos crimes resultam em diferentes tipos de evidência, e, por isso, cada caso deve ser tratado unicamente. Verifica-se, como exemplo,

o caso de acesso não autorizado, onde o perito deverá procurar por arquivos log, conexões, e por compartilhamentos suspeitos, ao passo que, em casos de pornografia, é feita a busca por imagens armazenadas no computador, histórico dos sites visitados recentemente, arquivos temporários, dentre outros.

A lei Carolina Dieckmann, também conhecida como a Lei Brasileira 12.737/2012, proporcionou uma mudança no código Penal brasileiro (Decreto-Lei2.848) que, tipificou os crimes informáticos. Este projeto de lei deu-se a partir do momento em que trinta e seis fotos íntimas, inclusive conversas pessoais da atriz Carolina Dieckmann, foram divulgadas pela internet sem a sua autorização.

Desse modo, as etapas que um perito forense deve seguir são as referentes ao ciclo de investigação:

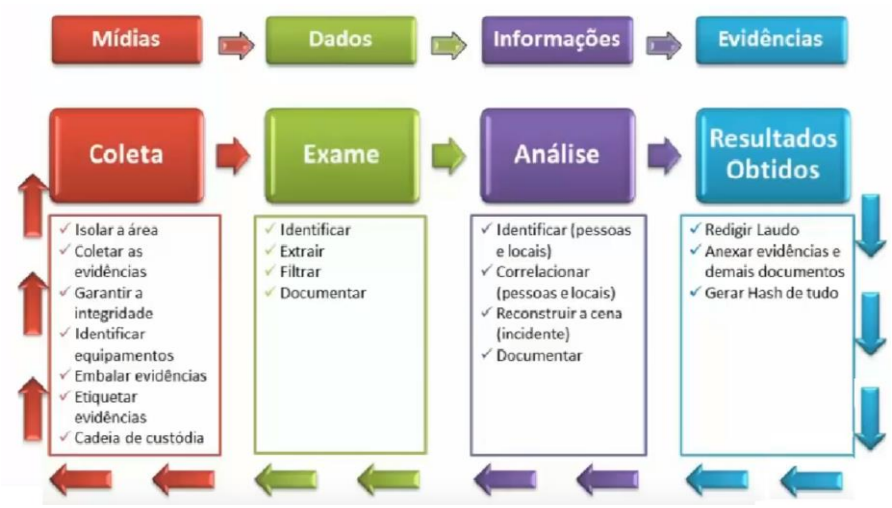

Figura 1 http://fdtk.com.br/wiki/tiki-index.php?page=Inicial

Antes de começar o estudo sobre perícias digitais em si, vale fazer algumas observações sobre o tema da investigação forense computacional, do ponto de vista jurídico.

Araújo (2010), diz que as provas colhidas durante um inquérito devem ser preservadas, em prol de seu aproveitamento no processo judicial. Isso seria dizer que, durante uma investigação forense computacional, algumas regras devem ser observadas.

Primeiro, o sistema investigado deve ser protegido de qualquer tipo de manipulação durante a operação, se possível, é recomendado possuir uma cópia do disco rígido, identificar, bem como, recuperar, todos os arquivos e aplicativos instalados, inclusive aqueles que tinham sido excluídos.

Também é importante fazer uma avaliação do sistema, identificando os acessos, cópias ocultas, protegidas, e arquivos temporários. Sendo assim, o monitoramento de fatores gerais relativos à atividade dos usuários é de extrema valia, visto que, na

atualidade, por meio dos equipamentos eletrônicos, trona-se possível a disponibilização e consulta a todos os tipos de informação sempre que se desejar e em qualquer lugar, uma vez que, atualmente, há o acesso a meios velozes e de fácil uso.

Além disso, constata-se constantes usos dos serviços disponíveis pela internet, que possibilitam a ampliação e otimização de sua infraestrutura, mas, também existem cada vez mais *softwares* com finalidades ilícitas, que podem ser utilizados e acessados facilmente, trazendo consigo um crescimento significativos de invasões em computadores (MELO, 2009).

Por este motivo a internet pode ser utilizada universalmente, tanto por pessoas com objetivos variados, do aprendizado ao entretenimento, quanto para a prática de crimes.

É inegável que pelo o uso de meios eletrônicos para atos ilícitos, e consequente, para obter-se de provas dos mesmos, estes fatores ainda carecem de estudos, técnicas aperfeiçoadas e regulamentação legal, e, com o objetivo de auxiliar e esclarecer tais investigações, é que surgiu a disciplina da computação forense.

4. Ferramenta de software

As ferramentas de perícia são importantes, pois, ajudam os peritos e auxiliam no processo de investigação. Existem dois tipos de perícia, as de *hardware* e as de *softwares*, e, no que se refere a este trabalho, tomou-se como exemplo as ferramentas de *software*.

Existem várias ferramentas que realizam a captura e a análise de informações de um smartphone, porém, a maioria destas são softwares de foco comercial. Existem ainda alguns exemplos de softwares não comerciais, um deles é a *Santoku Linux,* que foi criada a partir de três empreendimentos: a forense móvel, que possui versões gratuitas e ferramentas de imagem para *NAND*, cartões de mídia e *RAM*; a *Malware* para dispositivos móveis que possui uma ferramenta de descompilação e desmontagem, bem como, o terceiro empreendimento que é o acesso a bancos de dados de *malware*.

Abaixo, tem-se um exemplo do teste realizado por meio de uma das possíveis ferramentas, no caso, *AFLogical:*

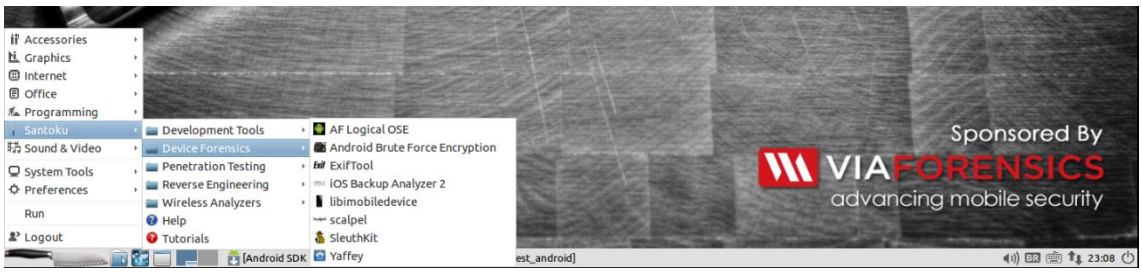

Figura 2 Próprio autor

Nesta imagem, está sendo executado a *AFlogical* com o emulador android.

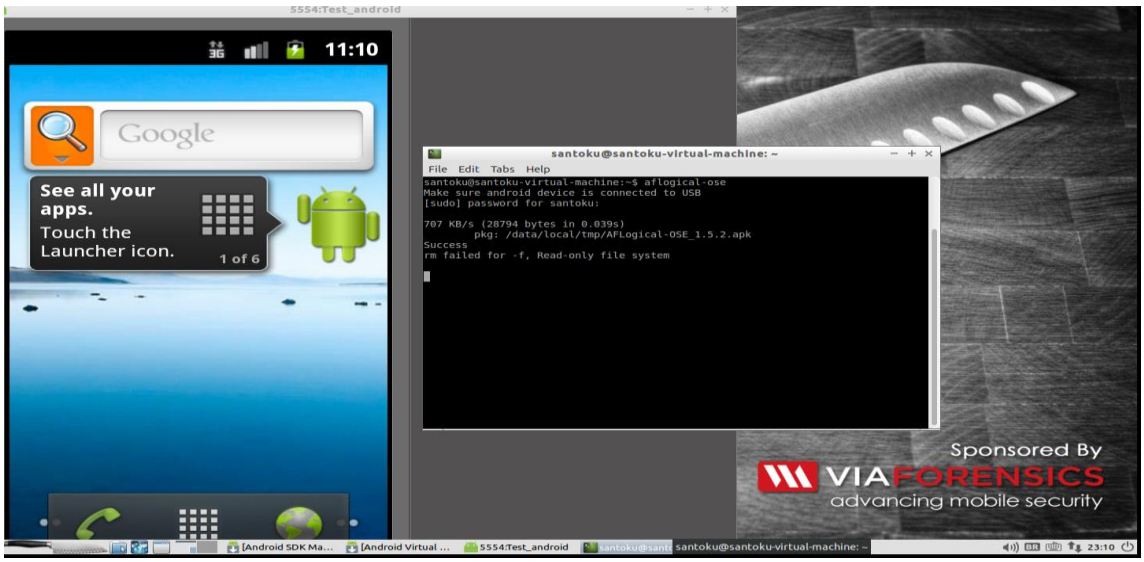

Figura 3 Próprio autor

Aqui, temos a captura dos dados do emulador.

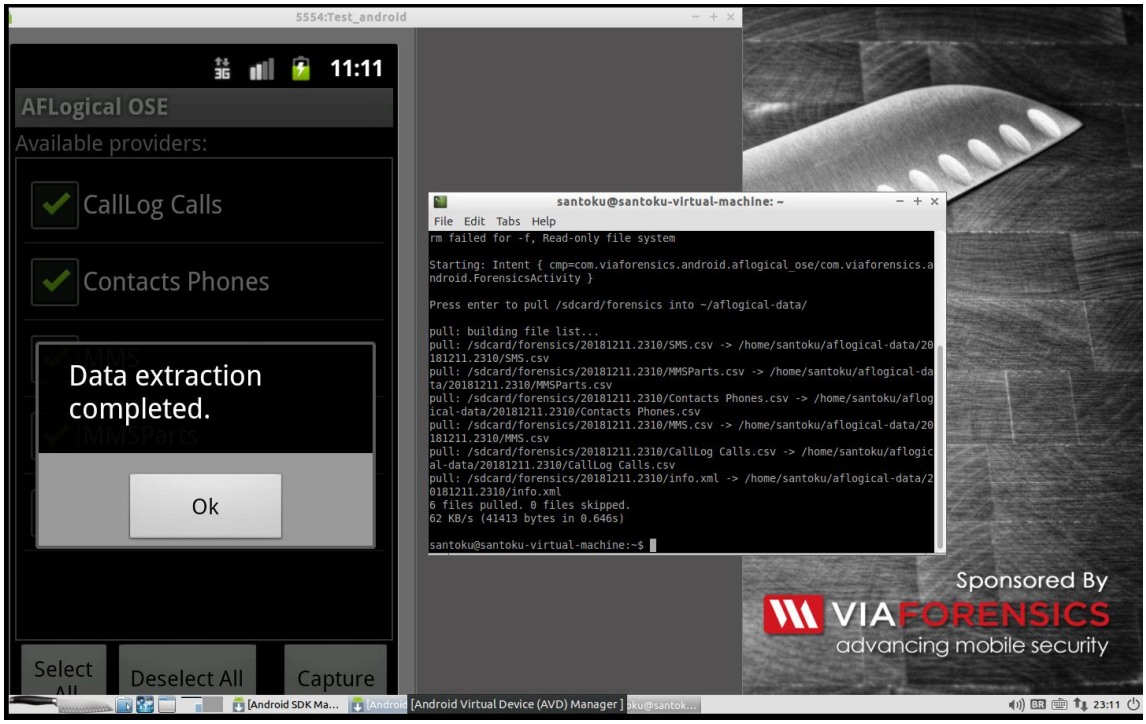

Figura 4 Próprio autor

Já nesta imagem, tem-se como exemplo as ligações de um lado, e, do outro lado, os dados capturados mostrando as ligações feitas.

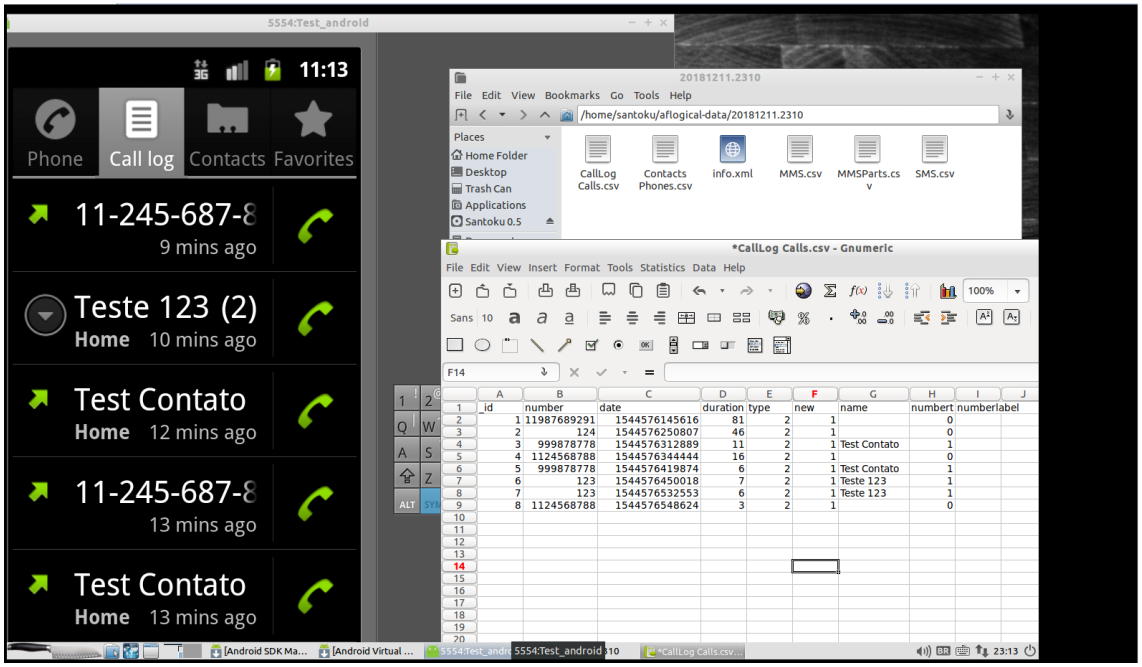

Figura 5 Próprio autor

Nesta imagem vemos as mensagens e os contatos de demonstração.

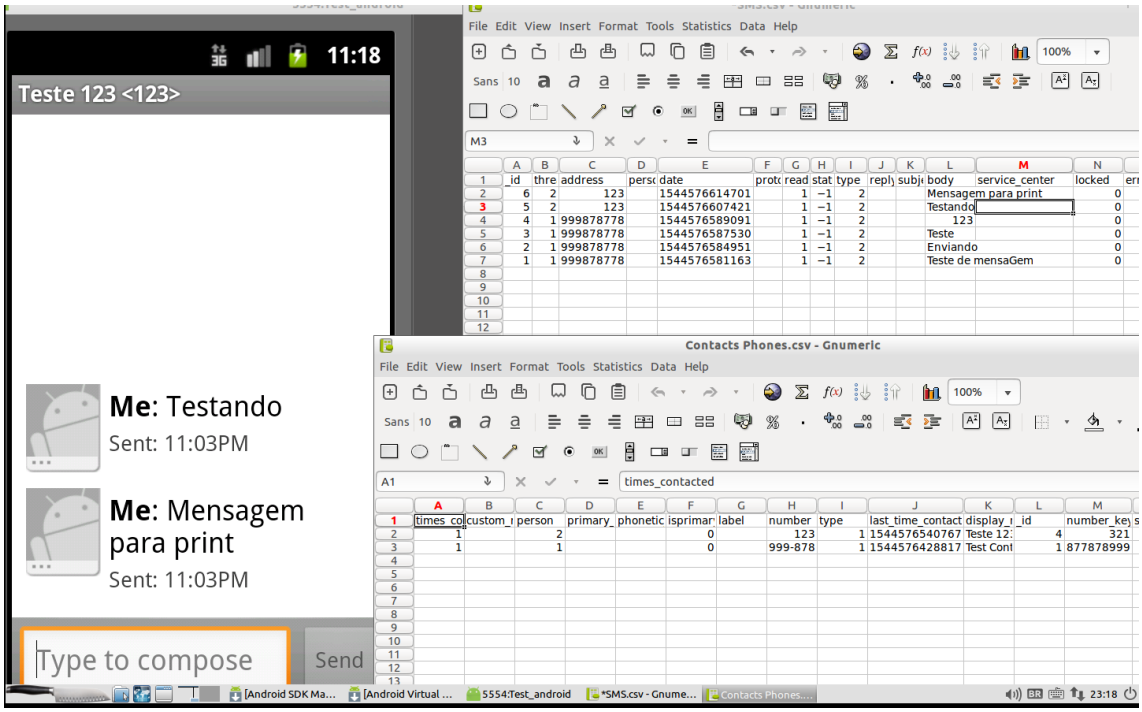

Figura 6 Próprio autor

A imagem a seguir apresenta os contatos, ligações e sms de um aparelho celular privado. Obs: alguns dados foram obstruídos em prol da segurança dos dados do dono do telefone.

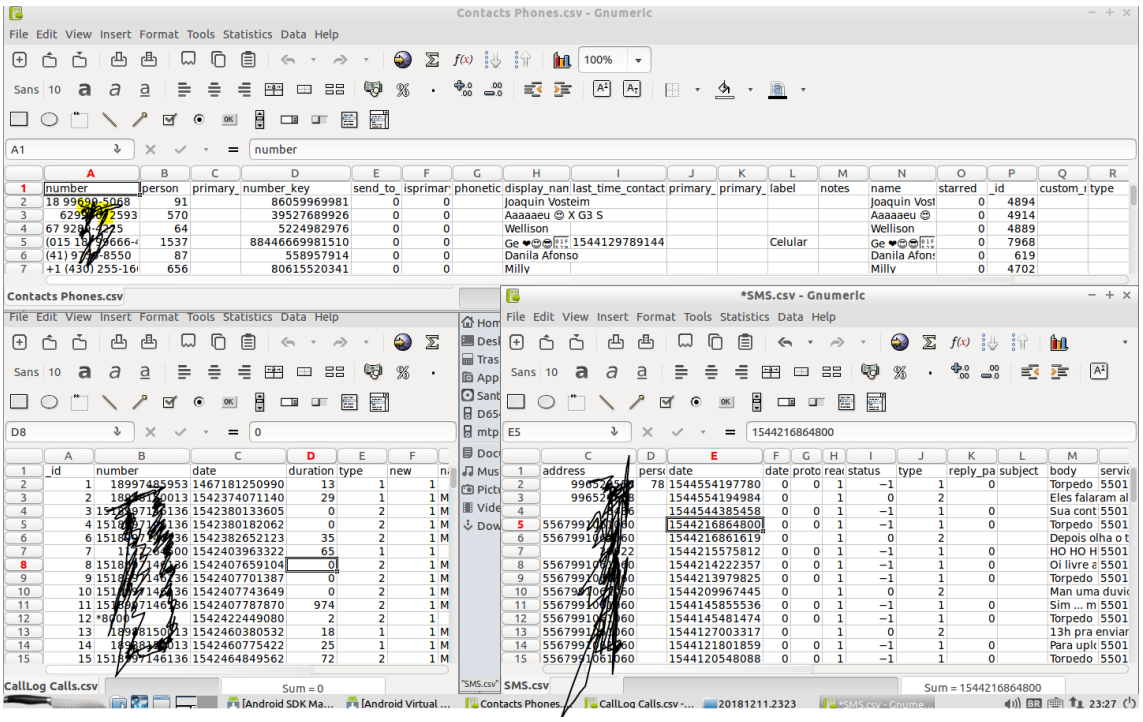

Figura 7 Propio autor

Por fim, pode-se afirmar que através da distribuição Linux *Santoku*, que possui várias ferramentas de perícia, foi possível capturar os dados de determinado aparelho celular. Isso significa que, a análise dos dados, pode ser otimizada por causa da agilidade de dada distribuição, que em menos de um segundo captura todas as informações privadas do aparelho celular, como vimos nos exemplos demonstrados acima.

5. Conclusão

Neste estudo, buscou-se por ferramentas que realizassem uma análise forense em dispositivos móveis, de modo a elucidar como os processos exigem um maior conhecimento de técnicas por parte do analista que tem como objeto, um dispositivo *mobile*. Aqui foram utilizados apenas uma das possibilidades de obter-se os dados, mas, existem outras, como por exemplo a *autopsy*, dentre outros.

Vale destacar que, os dados pessoais foram facilmente encontrados, como por exemplo, as data dos dispositivos, que possibilitaram uma análise de tudo aquilo que foi realizado no aparelho telefônico.

Mediante a obtenção dos resultados, percebeu-se que um dos maiores desafios da perícia em dispositivos móveis, com ferramentas *open source*, é que, os dispositivos precisam estar com a função ADB ativada, ao passo que o *root* pode estar habilitado ou não.

Cada dispositivo pode ser analisado de diferentes formas, e, por isso, o trabalho da perícia torna-se mais difícil. Além disso, os distintos padrões de bloqueio de tela, como por exemplo, bloqueio por meio de identificação biométrica, íris dos olhos, facial, entre outros, podem dificultar o andamento de uma investigação, visto que, para ativação da função e depuração USB (acesso ADB), o perito tem que ter acesso manual ao telefone celular.

Como sugestão, acredita-se que com o desenvolvimento de pesquisas futuras, será possível pensar na criação de ferramentas *open source* que possibilitem o processo de *rooting* nos dispositivos na mesma proporção que, viabilizem, no mesmo ambiente, a análise das partições escolhidas pelo perito. Sem dúvida, isso ajudaria o perito na obtenção mais rápida de resultados, otimizando a eficácia e conservação do dispositivo.

Sendo assim, foi possível encontrar uma ferramenta de baixo custo que fazia a análise do dispositivo da mesma maneira que uma ferramenta com foco comercial realizaria.

REFERENCIAS

ALBUQUERQUE, Roberto Chacon. **Criminalidade informática**. São Paulo: Editora Juarez de Oliveira, 2006.

ARAUJO, José Mariano de. **Cyber Crimes – Delegado Mariano. Weblog sobre crimes eletrônicos no mundo**. <http://mariano.delegadodepolicia.com/>. Acesso em: 8 de junho de 2010.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense**. 1. Ed. São Paulo: Novatec,2011.

FREITAS, Andrey Rodrigues**. Perícia Forense Aplicada à Informática**. Rio de Janeiro: Editora Brasport, 2006.

MELO, Sandro. **Computação Forense com Software Livre**. Rio de Janeiro: Alta Books, 2009. 1ª edição.

RUIZ, Luis Orlando Aponte. **Criminalística - Aspectos históricos e evolução no Estado de São Paulo**. Disponível em: <http://www.revistademedicinalegal.com.br/default.aspx?edicao=&secao=16&subsecao=45&indice=1&indiceSubsecao=1>. Acessado em: 20 nov. 2018

GONZÁLEZ, Elena Labajo. **Ciencias Antropológicas: la Antropología Forense**. Dez. 2004. Disponível em: <http://www.p3blog.net/index.php?cat=21>. Acessado em 20 nov 2018.

LUQUE, Bartolomé Luque Serrano. **Ciencia Forense: ¿cómo usar la ciencia y la tecnología para desvelar lo ocurrido?**. Todo-Ciencia.com. 2002 Disponível em:<http://matap.dmae.upm.es/WebpersonalBartolo/articulosdivulgacion/crimenes_3.htm>. Acessado em 20 nov. 2018

SECURITYFOCUS, S. G. Masood. **Malware Analysis for Administrators**: Disponível em: <http://www.securityfocus.com/infocus/1780 >. Acesso em: 20 nov 2018.

SHINDER, Debra Littlejohn. **Syngress Scene of Cybercrime: Computer Forensics Handbook**. Rockland: Syngress Publishing, Inc, 2002.

ZARZUELA, José Lopes**. Temas fundamentais de criminalística**. Porto Alegre: Sagra – Luzzatto, 1996

ZILLO NETO, Marcello. **Segurança da Informação e Tecnologia**. Disponível em: <http://mzillo.blogspot.com/>. Acesso em: 20 nov 2018.