SiCReT - Sistema de Cruzamento de Registros Telefônicos

Luiz Rodrigo Grochocki[1], Alexandre Vrubel[1], Raphael Laércio Zago[1], Alonso Decarli[2], Cinthia O. A. Freitas[2]

[1] Instituto de Criminalística do Paraná – Polícia Científica do Paraná
Av. Visconde de Guarapuava, 2652 – 80.010-100 – Curitiba – PR – Brasil

[2] Pontifícia Universidade Católica do Paraná – Escola Politécnica
Programa de Pós-Graduação em Informática (PUCPR/PPGIa)
R: Imaculada Conceição, 1155 – 80.215-901 – Curitiba – PR – Brasil

{luiz.grochocki, alexandre.vrubel, raphael.zago}@ic.pr.gov.br,
alonsodecarli@msn.com, cinthia@ppgia.pucpr.br

Abstract. *Information Science emerges as a tool able to revive the obsolete paradigms of law enforcement. Assuming that the crime labs hold a vast amount of computer forensics data, and trimming the edges of classical intelligence, police investigation and expert forensics, the integrated management of mobile forensics data through SiCReT is proposed. As a result it is expected that reports regarding cellphone examinations nurture a consolidated information database that allows in each examination report the analysis of properties and behavior of information on the forces governing the criminal flow, providing means to process and optimize the intelligence service, allowing the information sharing between all law enforcement agencies.*

Resumo. *A Ciência da Informação surge como ferramenta apta a revitalizar os obsoletos paradigmas da segurança pública. Partindo da premissa de que os órgãos de perícia detêm vasto banco de informações de computação forense, e aparando as arestas da inteligência clássica, da investigação policial, e do serviço pericial, propõe-se a gestão integrada de dados relativos a dispositivos computacionais por meio do Sistema de Cruzamento de Registros Telefônicos (SiCReT). Como resultado espera-se que laudos relativos a aparelhos telefônicos alimentem uma base de informações consolidada que aponte em cada laudo as propriedades e o comportamento da informação, as forças que governam o fluxo criminoso, fornecendo meios de processamento e otimização do serviço de inteligência, permitindo o uso por todas as forças de segurança pública.*

1. Introdução

O uso de computadores no Brasil continua crescendo de forma vertiginosa. Assim mostra a pesquisa divulgada em 2012, pela Fundação Getúlio Vargas (FGV), indicando que o número de computadores no Brasil dobrou nos últimos quatro anos, sendo que foi alcançada a marca de 99 milhões de máquinas em uso, somando-se PCs utilizados tanto em ambiente de trabalho quanto em casa[1]. E a tendência é que essa

[1] http://www.tecmundo.com.br/mercado/22359-brasil-possui-99-milhoes-de-computadores-em-

progressão se repita nos próximos três ou quatro anos. O trabalho da FGV também estima que em seis anos, 2018, a expectativa é de um computador para cada brasileiro [Meirelles 2013].

O mesmo fenômeno se observa com relação a telefones móveis, que segundo a Agência Nacional de Telecomunicações, em 2012, atingiu 250,8 milhões de linhas ativas de telefonia móvel [Anatel 2012].

Como a computação forense permeia as mais diversas áreas de perícia, seja trabalhando em conjunto, seja preparando a evidência para exame em outras áreas, o reflexo deste crescimento foi sentido no aumento crescente da demanda por exames envolvendo equipamentos computacionais e de telefonia.

O trabalho de Silva [Silva 2011] mostrou o volume de exames relacionados a Computação Forense no Estado do Paraná por meio do Sistema de Gerenciamento de Informações Periciais (SGIP), sendo possível dimensionar precisamente a crescente demanda por perícias na área de computação forense.

Levando-se em consideração o que foi exposto, a Seção de Computação Forense do Instituto de Criminalística do Paraná organizou o gráfico, apresentado na Figura 1, no qual se pode observar que a tendência é o crescimento vertiginoso e que os dispositivos computacionais tornem-se cada vez mais portáteis, acompanhando a mobilidade do usuário.

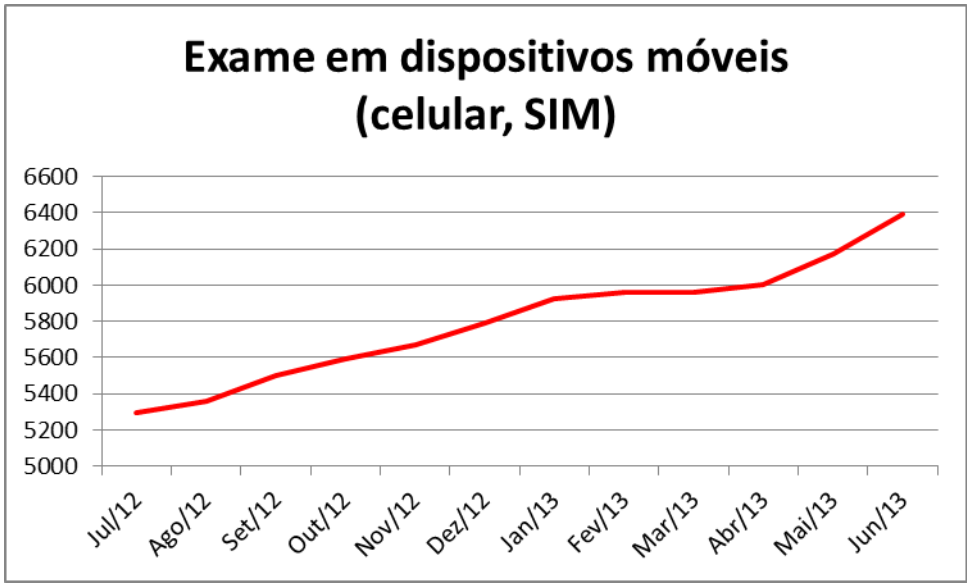

Figura 1. Gráfico de Histórico de CELULARES em Estoque – Janeiro à Julho/12

Tem-se, portanto, que a Ciência da Informação está definitivamente na ordem do dia, materializada através de ferramentas como os Serviços de Inteligência e Policiamento Preditivo aptos para revitalizar os obsoletos paradigmas da segurança pública brasileira. Assim, partindo das premissas de que a Seção de Computação Forense do Instituto de Criminalística do Paraná detém vasta base de informações de computação forense, que detém *expertise* para consolidação dos dados informacionais, frente a necessidade de ferramentas de Ciência da Informação, e aparando as arestas da inteligência clássica, da investigação policial, e do serviço pericial, propõe-se a gestão integrada de dados relativos a dispositivos computacionais por meio de um Sistema de Cruzamento de Registros Telefônicos - SiCReT.

Com esta onipresença da computação no dia a dia das pessoas a Seção de Computação Forense do Instituto de Criminalística do Paraná, com seu acervo de milhares de dispositivos computacionais torna-se uma fonte de dados e investigação de inteligência riquíssima e imprescindível para manutenção da Justiça que carece de consolidação de dados, evidências e provas, sejam estas físicas, eletrônicas, digitais ou virtuais.

Este artigo está organizado de tal forma que a Seção 2 traz uma breve introdução aos aspectos da computação forense e computação ubíqua, os quais estabelecem os fundamentos do sistema SiCReT. A Seção 3 descreve a proposta do sistema SiCReT. Na Seção 4 encontram-se descritos os motivos pelos quais o cruzamento de dados extraídos de celulares, dispositivos móveis, tem caráter importante para as demais áreas da Polícia Científica e, também, para a Segurança Pública. Finalmente, a Seção 5 aborda as considerações finais sobre o sistema SiCReT.

2. Computação Forense e Computação Ubíqua

A área denominada de computação forense ou forense computacional ou informática forense (*computer forensic*) envolve a extração, identificação, preservação e documentação de evidências digitais a partir de dados e informações armazenadas em mídias: magnéticas, ópticas ou eletrônicas. Para Michaud [Michaud 2001] a computação forense pode ser definida como uma peça do quebra-cabeça da investigação.

Assim, tal área do conhecimento se preocupa em estabelecer métodos e técnicas que podem ser resumidos nos três A's descritos, a saber [Kruse e Heiser 2002]: 1) Adquirir as evidências sem alterar ou causar danos aos dados originais, 2) Autenticar que as evidências coletadas são exatamente iguais aos dados originais e 3) Analisar os dados sem modificá-los.

Muitas são as situações nas quais a computação forense se faz necessária e urgente, podendo-se citar entre os crimes praticados por computador, os seguintes problemas: aliciamento de menores [Santin et al. 2012], pornografia infantil, fraudes bancárias, e-mail caluniosos, compartilhamento de *software*, música, filme e muitos outros [Nogueira 2009].

Deste modo, tais problemas necessitam da comprovação dos fatos que possam ser trazidos em juízo para as devidas responsabilizações. Portanto, o presente artigo está relacionado com aspectos técnicos e jurídicos da produção antecipada de provas digitais por meio da caracterização de boas práticas para que os três A's (adquirir, autenticar e analisar) possam ser garantidos.

Na Publicação Especial 800-101 do NIST [Jansen e Ayers 2007] os autores sugerem que a chave para o sucesso é a compreensão das características de *hardware* e *software* dos telefones celulares. Os dados dos assinantes e suas atividades por meio de celulares são muitas vezes uma fonte valiosa de provas em uma investigação. A maioria dos celulares tem um conjunto básico de características comparáveis entre diferentes aparelhos, tais como: microprocessador, memória ROM, memória RAM, módulo de rádio, processador de sinal digital, alto falante, tela, sistema operacional, bateria, PDAs, GPS, câmera, entre outros recursos.

Os autores explicam que a aquisição de dados a partir de um dispositivo pode ser física ou lógica [Jansen e Ayers 2007]. A aquisição física tem vantagens sobre a

aquisição lógica, uma vez que permite que os arquivos apagados e alguns dados restantes possam ser examinados, por exemplo, na memória não alocada ou em espaço do sistema de arquivos. Recomenda-se sempre fazer a aquisição de dados física antes da aquisição lógica. As ferramentas forenses adquirem informações dos dispositivos sem alterar o conteúdo, ou seja, em modo somente de leitura, e em geral geram *hash* (MD5, SHA) que garantem a integridade dos dados.

Investigações digitais são comparáveis às cenas de crime, comentam os autores [Jansen e Ayers 2007], visto que técnicas de investigação utilizadas pela aplicação da lei têm sido aplicadas como base para a criação de procedimentos utilizados quando se trata de evidências digitais.

Assim, cabe destacar tal qual [Jansen e Ayers 2007] estabelecido pelos Princípios de Probatória, os quais consideram que a prova digital tem dois aspectos: os componentes físicos, periféricos e mídia, que podem conter dados, e os dados extraídos a partir dessas fontes. Portanto, os autores sugerem que sejam respeitados quatro princípios ao trabalhar com evidências digitais, que podem ser resumidos de modo que: a) ações realizadas por investigadores/peritos não devem alterar dados contidos em dispositivos digitais ou em mídias de armazenamento que podem posteriormente ser solicitados perante o Juiz; b) indivíduos que acessam dados originais devem ser competentes para fazê-lo e ter a capacidade de explicar suas ações, visto que tais procedimentos são questionáveis pelas partes ou em juízo; c) uma cadeia de custódia deve ser estabelecida, bem como o registro de todos os procedimentos realizados, de maneira que se possa garantir a replicação dos resultados por um terceiro independente, sendo que toda documentação deve ser criada e preservada, documentando-se cada passo investigativo/pericial; d) a pessoa encarregada da investigação tem a responsabilidade geral de assegurar os procedimentos já mencionados e se os mesmos serão ou foram seguidos em conformidade com os métodos científicos e as leis vigentes.

De um modo geral, os autores [Jansen e Ayers 2007] abordam que os exames periciais muitas vezes revelam não apenas dados potencialmente incriminatórios, mas também informações úteis, tais como senhas, nomes de *login* na rede e atividades via Internet. Alguns dados também podem fornecer a ligação a outras fontes potenciais de provas mantidas em outros lugares, especialmente pelos prestadores de serviços de rede. Além de evidências diretamente relacionadas a um incidente, informações relevantes sobre a vida de suspeitos, de seus colaboradores, e os tipos de atividades em que eles estão envolvidos pode ser de grande valia ao procedimento investigatório/pericial.

Cabe ressaltar que será o Laudo Pericial que apresentará todo o conjunto de evidências, bem como, um detalhamento de todos os passos realizados e, ainda, as conclusões alcançadas pelas análises realizadas. Assim, os laudos dependem da manutenção de um registro cuidadoso de todas as ações e observações, descrevendo os resultados dos testes e exames, e explicando as inferências extraídas sobre o objeto de prova. Um bom laudo, ressaltam os autores [Jansen e Ayers 2007], se baseia em uma sólida documentação, anotações, fotos e dados extraídos, física e logicamente, por meio das ferramentas forenses.

Outro ponto relevante é a tendência mundial dos computadores estarem presentes no dia a dia das pessoas. Neste sentido, tem-se a Computação Ubíqua, oriunda do termo em inglês *Ubiquitous Computing* ou *Ubicomp* [Weiser 1993].

A Computação Ubíqua[2], também chamada de Computação Pervasiva ou Inteligência Ambiental [Moutinho 2010], descreve a presença direta e constante da informática e tecnologia na vida das pessoas, em suas casas e ambientes de convívio social. O objetivo da Computação Ubíqua é integrar totalmente a relação tecnologia/máquina com os seres humanos, de forma tal que seja invisível, no sentido de automático (utilizar sem perceber). Os computadores fazem parte da vida das pessoas de tal maneira que se tornam "humanos", com seus sistemas inteligentes, que os tornam onipresentes [Rolins 2001].

Tudo começou com um artigo publicado por [Weiser 1991], pesquisador da Xerox PARC, no qual ele enuncia que "*specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one Will notice their presence*". Para [Moutinho 2010] o termo "ubíquo" é usado para explicar que não somente os computadores estão presentes em qualquer lugar, mas toda a área de computação, embutidos nas estruturas básicas e fundamentais da vida do ser humano. Sabe-se também que a ubiqüidade é a propriedade daquilo que está presente em todos os lugares ao mesmo tempo, ou seja, algo onipresente [Bueno 2007].

Assim, tem-se que os dispositivos móveis podem ser encontrados e recuperados nas mais variadas situações suspeitas e que necessitam ser investigadas, para que a área da criminalística possa utilizar das informações contidas nestes dispositivos para compor ou esclarecer, por exemplo, um crime.

3. O Sistema SiCReT

A Computação Forense e a Computação Ubíqua estabelecem a base teórica e formal para o sistema SiCReT, de modo que se possa não somente organizar e padronizar a aquisição e análise de dados digitais extraídos de dispositivos móveis (celulares), mas também permitir o cruzamento de todo o conjunto de dados.

A ideia central deste sistema é que todos os laudos relativos a aparelhos telefônicos alimentem uma base de informações consolidada que apontem e investiguem em cada laudo as propriedades e o comportamento da informação, as forças que governam o fluxo criminoso, e os forneça meios de processamento e otimização do serviço de inteligência, permitindo a acessibilidade, alimentação e uso por todas as forças de segurança pública. A Figura 02 exemplifica o sistema SiCReT de modo a possibilitar uma visão geral, bem como, as fontes geradoras de informações e os atores intervenientes junto ao sistema.

Os métodos e técnicas estudados e a serem empregados no desenvolvimento do sistema SICReT estão relacionados com as seguintes áreas do conhecimento: Computação Forense, Descoberta do Conhecimento e Aprendizagem de Máquina e, ainda, Segurança de Sistemas Computacionais.

Assim, o projeto partirá da aquisição dos dados digitais a partir dos celulares, sendo que estão sendo estudados os métodos e *hardware*/*software* utilizados pelo Instituto de Criminalística do Paraná, a saber: Cellebrite UFED[3] e Microsytemation XRY[4]. Ambos realizam a extração de dados em padrão XML (*eXtensible Markup Language*), padrão este que permite descrever diversos tipos de

[2] http://neei.uevora.pt/~jay/cubi/
[3] http://www.cellebrite.com/pt/mobile-forensic-products/ufed-touch-ultimate.html
[4] http://www.msab.com/xry/what-is-xry

dados, de forma padronizada, facilitando o compartilhamento e indexação em um sistemas de informações.

A Tabela 01 exemplifica informações gerais da captura de dados em dispositivos móveis, com base no *hardware*/*software* Cellebrite UFED. A partir de todo o conjunto de dados pode-se então analisar quais dados permitirão a realização do cruzamento de informações provenientes de celulares distintos. Sabe-se *a priori* que são importantes para o cruzamento os dados contidos nas chamadas (realizadas e recebidas), mensagens de texto SMS (enviadas e recebidas), agenda de contatos, e número da linha telefônica. Alguns modelos de *smartphones* fornecem dados de mensagens eletrônicas (*e-mail*), salas de bate-papo (*chat*), entre outros. O projeto realizará e definirá o conjunto mínimo de atributos necessário ao cruzamento dos dados.

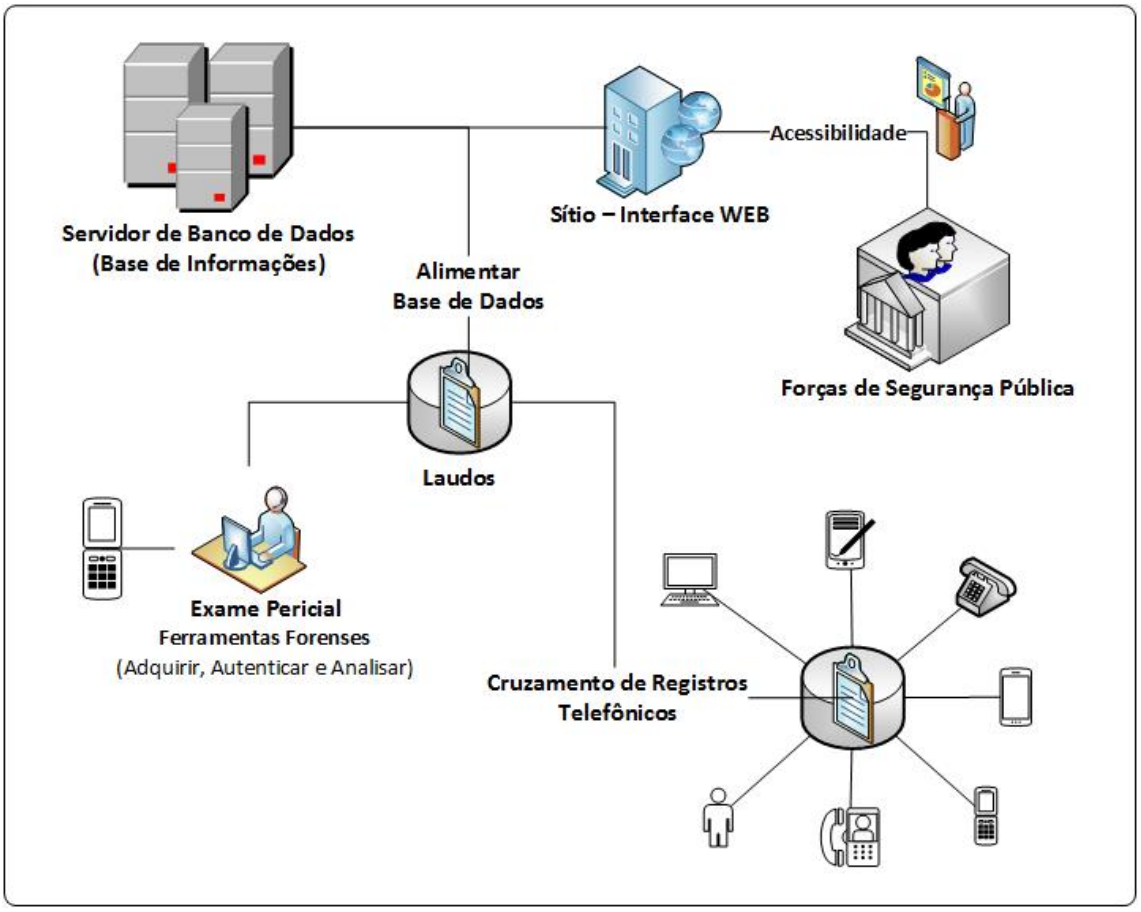

Figura 2. Proposta do Sistema SiCReT

Atualmente a base de dados da Seção de Computação Forense do Instituto de Criminalística do Paraná da Polícia Científica do Paraná – Curitiba encontra-se em formato .odt (*OpenDocument Text*) que é o formato de documento do Open Office. Ou seja, o sistema deve ser capaz de fazer uma busca e recuperação no arquivo de dados e, então, instanciar um banco de dados relacional de modo a contribuir para a preparação dos laudos técnicos dos peritos.

A fim de permitir o cruzamento e recuperação das informações registradas (e possivelmente a inserção de novos dados) faz-se necessário o uso de um sistema de informações baseado na Web (Internet e Intranet), desta forma, o banco de dados não demandará sincronização entre diferentes locais e será possível o acesso remoto ao

mesmo. A utilização de tecnologia Web permitirá também um melhor acompanhamento e preservação da segurança das informações armazenadas.

Cabe salientar que a privacidade dos indivíduos envolvidos será preservada e a segurança do sistema como um todo contará com métodos de criptografia assimétrica (algoritmo SHA-2 - *Secure Hash Algorithm*), sendo que todo o tráfego de dados via interface Web será criptografado. Além disto, o sistema contará com identificação de usuários (senha, login e biometria) e, ainda, contará com a criptografia da infra-estrutura do sistema servidor e também do sistema gerenciador de banco de dados. Sob a ótica da segurança computacional, o sistema controlará o acesso e a inserção de informações por meio de usuários, de modo a registrar as operações realizadas pelos usuários, permitindo estabelecer "quem" realizou "o quê" no sistema.

O sistema conta com um filtro já desenvolvido pela Seção de Computação Forense do Instituto de Criminalística do Paraná da Polícia Científica do Paraná – Curitiba para converter automaticamente os dados extraídos em padrão XML para os laudos periciais. Este filtro tem por base o LibreOffice (que é uma suíte de escritório, livre e compatível com as principais suítes de escritório do mercado. Oferece todas as funções esperadas de uma suíte profissional: editor de textos, planilha, apresentação, editor de desenhos e banco de dados) e o formato XSLT (*eXtensible Stylesheet Language for Transformation*), a qual é uma linguagem de marcação XML usada para criar documentos XSL que, por sua vez, definem a apresentação dos documentos XML no *browser* e outros aplicativos que a suportem, como apresentado pelo perito criminal Alexandre Vrubel na VIII Conferência Internacional de Perícias em Crimes Cibernéticos [Vrubel 2011].

TABELA 1 - Informações Gerais da Captura

Parâmetros
Fabricante selecionado
Modelo selecionado
Fabricante detectado
Modelo detectado
Revisão
Nome do equipamento
IMEI (*International Mobile Equipment Identity*)
Número de série
ICCID (*International Circuit Card ID*)
IMSI (*International Mobile Subscriber Identity*)
Endereço Bluetooth
Endereço Wi-Fi
Início da extração
Fim da extração
Data/Hora do telefone
Tipo de conexão
Extração suportada para Agenda Telefônica, SMS, Chamadas, MMS, *email*, Imagens, Toques, Áudio, Vídeo, Calendário, Tarefas, Anotações

Deste modo, tem-se que o desenvolvimento do sistema SiCReT seguirá uma linha metodológica embasada na pesquisa experimental, por meio da proposição de um sistema computacional, desenvolvimento de protótipo com validação e testes.

4. Cruzamento de Dados de Dispositivos Móveis

Cabe destacar como e porque o cruzamento de dados extraídos de celulares, dispositivos móveis, tem caráter importante para as demais áreas da Polícia Científica e, também, para a Segurança Pública.

Inicialmente, pode-se estabelecer um banco de informações relativo a dados extraídos de dispositivos computacionais coletados em locais de crime visto que um local de crime fornece uma grande variedade de evidências, as quais podem estar relacionadas com outros crimes ou criminosos [Dorea et al. 2003].

Além disto, o armazenamento e recuperação de dados relativos à identidade de indivíduos e seus respectivos registros telefônicos (ligações, mensagens e agenda) podem auxiliar no entendimento da criminalística dinâmica, bem como, no estabelecimento do nexo causal. Tais elementos são de suma relevância visto que o perito somente poderá concluir ou fazer qualquer afirmação por meio do laudo, se puder fundamentar suas assertivas com uma justificativa técnico-científica [Rosa 1999].

Em termos de consultas e relacionamentos entre casos sob investigação, cabe destacar que o sistema permitirá emitir o rol de laudos que tenham relação, por exemplo, com um novo caso. Permitirá também consulta simples por números de linhas telefônicas ou indivíduos já cadastrados no sistema. E, ainda, será possível correlacionar registros de diferentes indivíduos a fim de estabelecer vínculos entre os mesmos.

No que tange a emissão de resultados impressos e gráficos, o sistema SiCReT prevê a geração de relatórios de vínculos entre indivíduos organizados por par ou por grupo, a geração de grafos globais de relações entre indivíduos/números de linhas telefônicas. Permitindo, ainda, a elaboração de mapeamento geográfico da área de atuação dos indivíduos suspeitos, estabelecendo o georreferenciamento e respectivos mapas de atos criminosos. Deste modo, será possível identificar quadrilhas e chefes de organizações criminosas por meio do cruzamento de dados.

Ressalta-se que o sistema vem sendo desenvolvido e testado em condições reais (não simulado) visto que Seção de Computação Forense do Instituto de Criminalística do Paraná dispõem de dados para realização dos testes e, conseqüentemente, da validação do sistema.

Finalmente, espera-se ainda que o sistema SiCReT possa auxiliar por meio de filtros de pesquisa, relacionando os números de linhas telefônicas ou indivíduos com, por exemplo, tipos de entorpecentes, armas utilizadas e/ou encontradas em cenas de crime (ou locais de morte), estabelecendo quando possível a região de atuação. Na verdade, não se localizou na literatura técnico-científica [Ayres et al. 2005] [Carrier 2005], até o presente momento, sistemas que contemplem o cruzamento de dados entre dispositivos distintos, somente ferramentas (*hardware*/*software*) para extração de dados e análise de celulares isoladamente.

5. Conclusão

A Ciência da Informação, Sistemas Inteligentes e o Policiamento Preditivo estão definitivamente na ordem do dia dos operadores de ares de Segurança Pública. Existe um clamor por órgãos de Segurança Pública que trabalhem de forma planejada, eficiente e ágil, primando pelo tratamento da causa e não só do efeito. Neste sentido, o Sistema de Cruzamento de Registros Telefônicos - SiCReT, a exemplo dos sistemas

SisBala (Sistema de Indexação Balística) [Figueiredo 2012] e CODIS (*Combined DNA Index System*)[5], irá contribuir significativamente para aumentar a qualidade dos serviços prestados pela área de Segurança Pública, pois a cada laudo emitido pelos órgãos de perícia, o mesmo será tratado de forma sistêmica e como parte de um todo analisado com base em todo o potencial técnico-científico. Além disto, o SiCReT é uma oportunidade para relacionar conhecimentos das áreas de Computação Forense, Descoberta do Conhecimento, Aprendizagem de Máquina e Segurança de Sistemas Computacionais.

6. Referências

Anatel – Agência Nacional de Telecomunicações, "Em março, telefonia móvel ultrapassa 250 milhoes de linhas ativas", 2012. Disponível em http://www.anatel.gov.br/Portal/exibirPortalNoticias.doacao=carregaNoticia&codigo=25164 Acesso em: 01 de agosto de 2013.

Ayres, R.; Jansen, W.; Cilleros, N.; Daniellou, R.. "Cell Phone Forensic Tools: An Overview and Analysis". National Institute of Standards and Technology – NIST, NISTIR 7250, 2005, 176p. Disponível em <http://csrc.nist.gov/publications/nistir/nistir-7250.pdf> Acesso em: 01 de agosto de 2013.

Bueno, S.. "Minidicionário da Língua Portuguesa". 2ª. Edição, São Paulo: FTD, 2007. 830p.

Carrier, B.. "File System Forensic Analysis". Addison Wesley Professional, 2005. 382p.

Craiger, J.P.. "Computer Forensics Procedures and Methods". To appear in H. Bigdoli (Ed.), Handbook of Information Security. John Wiley & Sons, 2007.

Dorea, L.E.C.; Stumvoll, V.P.; Quintela, V. "Criminalística". Campinas, SP: Millennium, 2a. Edição, 2003. 277p.

Figueiredo, T.. "Sisbala: A solução para as armas ainda não periciadas no país". Revista; Perícia Federal, APCF, Ano XIII, No. 29, 2012. p.14-15.

Jansen, W.; Ayers, R.. "Computer Security - guidelines on cell phone forensics", National Institute of Standards and Technology – NIST, Special Publication 800-101, May 2007, 104 p. Disponível em <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf> Acesso em: 01 de agosto de 2013.

Kruse, W.G.; Heiser, J.G.. "Computer forensics: incident response essentials". Indianapolis: Addison-Wesley, 2002.

Meirelles, F.S.. "24ª Pesquisa Anual do Uso de TI", FGV-EAESP-CIA, 2013, Disponível em <http://eaesp.fgvsp.br/sites/eaesp.fgvsp.br/files/arquivos/gvpesqti2013ppt.pdf> Acesso em 01 de agosto de 2013.

Michaud, D.J.. "Adventures in Computer Science". SANS Institute, 2001.

Moutinho, A.M. "Inteligência Ambiente: contributo para a conceptualização de parede inteligente". Dissertação de Mestrado, Universidade de Lisboa, 2010. Disponível em

[5] http://www.fbi.gov/about-us/lab/biometric-analysis/codis

<http://repositorio.ul.pt/bitstream/10451/7277/2/ULFBA_tes%20392.pdf> Acesso em 03 de abril de 2013.

Nogueira, S.A. "Crimes de Informática". Leme: BH Editora e Distribuidora, 2ª. Edição, 2009. 624p.

Rolins, C.V.A.N.. "Aplicações para Computação Ubíqua". Programa de Mestrado, Departamento de Informática, PUC-Rio. 2001. Disponível em <www-di.inf.puc-rio.br/~endler/courses/Mobile/.../01> Acesso em 03 de abril de 2013.

Rosa, M.V.F.. "Perícia Judicial: teoria e prática". Porto Alegre: Sergio Antonio Fabris Editor, 1999. 295p.

Santin, P. L. L.; Freitas, C. O. A.; Paraíso, E.C.; Santin, A.. "Modelagem de Aliciamento de Menores em Mensagens Instantâneas de Texto". In: XII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2012), SBC, 2012. v. 1. p. 288-301.

Silva, M.V.. "SGIP – Sistema de Gerenciamento de Informações Periciais". In: XXI Congresso Nacional de Criminalística, 2011.

Vrubel, A.. "Using XSLT Filters to Improve Productivity and Quality on Cell Phone Forensics". In: 6th International Conference on Forensic Computer Science (ICoFCS2011), 2011. p. 132-136.

Weiser, M.. "The Computer for the 21st Century". Scientific American, set., 1991. p. 94-104.

Weiser, M.. "Some Computer Science Issues in Ubiquitous Computing". Communications of the ACM, July,1993. (reprinted as "Ubiquitous Computing". Nikkei Electronics; December 6, 1993; pp. 137-143.) Disponível em <http://www.ubiq.com/hypertext/weiser/UbiCACM.html> Acesso em: 03 de abril de 2013.

