ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES A LOS AUTORES

Vol. 38 (Nº 51) Ano 2017. Pág. 25

O uso da informática na perícia criminal e suas ferramentas

The use of computer science in criminal expertise and its tools

Kiulyn Fernandes Taborda SCHMITZ 1; João Eduardo Branco de MELO 2; Vanilson CARDOSO 3

Recebido: xx/06/2017 • Aprovado: xx/07/2017

Conteúdo

RESUMO:
Nos dias atuais, a tecnologia está presente em passo evolutivo graças às necessidades do ser humano em seu dia-a-dia, principalmente com maneiras de inovar e aprimorar os recursos utilizáveis, juntamente com a Criminalística através de soluções computadorizadas de envolvimento investigativo que visem à precisão e a solução de crimes. Neste trabalho, estuda-se a Computação Forense, sendo uma área referente à Ciência Forense, como um ramo criminalístico que envolve técnicas e ferramentas aplicadas à investigação e solução de crimes envolvendo meios eletrônicos.
Palavras-Chave: Criminalística; Computação Forense; Ciência Forense.

ABSTRACT:
Nowadays, technology is present in evolutionary step thanks to human needs in their day-to-day, especially with ways to innovate and improve the usable resources, along with criminalistics through computer solutions investigative involvement aimed at precision and solving crimes. In this paper, we study Computer Forensics, being an area related to Forensic Science, as a criminalistics branch involving techniques and tools applied to the investigation and solution of crimes involving electronic media.
Keywords: Criminal expertise; Forensic computer solution; Forensic Science

1. Introdução

No ramo da polícia científica, inúmeros são os métodos utilizados na Criminalística, na qual consiste no exercício da ciência forense através da utilização de técnicas apuradas, com o intuito da prevenção, esclarecimento ou solução geral de crimes. As técnicas utilizadas, serão realizadas por um perito responsável, no qual está encarregado na produção da perícia técnica conforme à natureza do delito, e por fim na confecção de um Laudo Pericial.

> "(...) a prova pericial é produzida a partir de fundamentação científica, enquanto que as chamadas provas subjetivas dependem do testemunho ou interpretação das pessoas,

> podendo ocorrer uma série de erros, desde a simples falta de capacidade da pessoa em relatar determinado fato, até o emprego de má-fé, onde exista a intenção de distorcer os fatos para não se chegar à verdade.” (ESPÍNDULA, 2002:22).

Ao longo dos anos, a ciência forense está evoluindo ao passo que os crimes sejam colocados em prática, de forma que se obtenha possíveis conclusões e que suas causas e efeitos sejam estudadas.

---

2. Informática na perícia criminal

A aplicação da informática na perícia criminal, pode estar diretamente relacionada à computação forense, uma área específica da ciência forense, e atuante no ramo militar, governamental e de inteligência, que segundo (ALTIMUS; KATEEB, 2014) a computação forense pode ser definida como formas de análises com o intuito de envolver a preservação, extração e documentação de evidências obtidas em mídias digitais, advinda de evidências digitais.

O papel da computação forense tem funções como de um processo investigativo, que conforme (SONNTAG, 2008), pode ser considerado a mistura entre elementos da Ciência da Computação e do Direito, tendo em foco a análise e coleta de informações de computadores, redes, dados de GPS, sistemas *wireless*, dispositivos de armazenamento (*pendrives*, HDs, celulares e afins) como solucionar e entender também as práticas relacionadas aos crimes cibernéticos e de informática, a fim de avançar os processos jurídicos, sendo passível de encaixe em penas legais conforme o delito praticado em questão obtido através de prova na perícia.

No Brasil todavia, em 2011 foi sancionada a lei nº 12.737 a partir do acréscimo no Decreto de Lei nº 2.848, de 7 de Setembro de 1940 do Código Penal, na qual específica o tratamento para crimes de delitos informáticos, nela os Art. 154-A e 154-B determinam:

> “Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. “(Lei nº12.737/11 – Código Penal Brasileiro, 2014).

Porém, caso não haja um crime de informática as punições possíveis decorrentes da perícia realizada poderão enquadrar-se no Código Penal Brasileiro, conforme for o delito praticado.

Exemplo: Tráfico de Drogas, no qual o indivíduo terá seu aparelho examinado, e caso haja provas de sua participação ou envolvimento no ato ilícito ele poderá ser enquadrado conforme o Art. 33 da Lei nº 11.343/06 (Lei de Tóxicos).

> “Art. 33. Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar: Pena - reclusão de 5 (cinco) a 15 (quinze) anos e pagamento de 500 (quinhentos) a 1.500 (mil e quinhentos) dias-multa.” (Lei nº 11.343/06 Lei de Tóxicos, 2006).

A computação forense na maioria dos casos estará diretamente ligada à polícia cientifica, sua prática será realizada por um perito, o qual utilizará de ferramentas e recursos específicos para a extração das informações que sejam necessárias para a confecção de um laudo pericial.

Nesta fase, a prudência e o conhecimento do perito farão papéis de extrema importância para a desenvoltura do processo criminal, visto que, o laudo deverá ser preciso e imparcial, assim sendo, no presente laudo, o perito deverá descrever de maneira formal, sucinta e objetiva todos os procedimentos e exames técnicos utilizados em sua perícia. (VELOSO DE FRANÇA, 2005) atesta que um perito deverá ser entendido como uma pessoa qualificada ou experiente no assunto ao qual esteja sendo tratado, visando, quando for solicitado esclarecer fatos que sejam de interesse da justiça.

2.1. Examinando a Evidência

Na computação forense segundo (POLLIT et al., 2000) uma evidência poderá ser representada por impressoras, chips e placas em geral, unidades centrais de processamento, meios de armazenamento e monitores, podendo ser facilmente descritos como uma unidade física. No entanto, as evidências, enquanto armazenadas nestes meios físicos, será latente e só existirá em um formulário eletrônico metafísico.

O processo de examinação fará com que a prova se torne visível e ao mesmo tempo explicará a sua origem e significância. Assim sendo, (NIJ, 2001) implica que na fase de examinação, várias coisas deverão ser realizadas.

Primeiro, deverá ser realizada a documentação do conteúdo e o estado da evidência em sua totalidade. Essa documentação permitirá que todas as partes descubram o que estará contido na prova. Neste processo a busca de informações que podem estar escondidas também é incluída.

Uma vez que toda a informação se torne visível, o processo de redução de dados pode começar, como uma prática de refinamento ou filtragem. Dada a enorme quantidade de informações que poderão estar armazenadas em uma mídia de armazenamento, esta parte é considerada fundamental. (NIJ, 2001). Todavia, (POLLIT et al., 2000) salienta que uma evidência nem sempre existirá de maneira isolada, esta evidência é um produto de dados armazenados criados através da utilização de um aplicativo.

2.2. Extraindo Evidências

Segundo (NIJ, 2004), a extração de uma evidência digital deverá ser cautelosa devido a sua fragilidade, ou seja, um manuseio ou examinação indevida, poderá acarretar no dano, alteração ou até mesmo destruição da evidência. Uma examinação decorrente de falhas cometidas pelo encarregado da perícia, poderão ser passíveis de conclusões imprecisas, sendo então altamente recomendado levar em consideração a preservação deste tipo de evidência. Todavia (POLLIT et al.,2000) argumenta que o maior desafio para a computação forense está em desenvolver métodos e técnicas que permitam a obtenção de resultados válidos e confiáveis ao mesmo tempo que protejam a evidência de um possível dano.

A extração de uma evidência digital será realizada a partir de uma utilização ampla de recursos, por meio de software, hardware ou ferramentas para este propósito. Deste modo, a extração de uma evidência poderá ser realizada através dos mais variados métodos.

2.2.1. Extração Lógica

A extração lógica, é constituída pela aquisição de dados em arquivos e diretórios a partir do sistema operacional do dispositivo, (MOOIJ, 2010) explica que a extração lógica pode ser realizada através de duas formas: Unidades Software-Hardware, ou Softwares próprios para a realização da extração lógica. Entretanto (BEN-MOSHE, 2012) ratifica que, por mais que a extração lógica passe a ser um processo consideravelmente rápido, de baixa complexibilidade, todavia leva a desvantagem na limitação de aquisição de dados, visto que, nesta prática não será possível a obtenção de dados apagados do sistema.

"A extração lógica implica extração de dados usando o sistema operacional do dispositivo através de um conjunto de comandos conhecido (por exemplo, comandos AT). Isto significa que as ferramentas de extração de dados se comunicam com o sistema operacional do dispositivo e solicitam as informações do sistema. Isso permite a aquisição da maior parte dos dados do dispositivo em tempo real." (CELLEBRITE MOBILE SYNCHRONIZATION LTD, 2014)

2.2.2. Extração Física

A extração física consiste de uma varredura seguida da aquisição de dados contidos na memória flash do dispositivo, sendo então realizada uma cópia minuciosa *(bit* a *bit*). (MURPHY,

2014) sintetiza, afirmando que a extração física também poderá ser chamada de aquisição física, ou senão despejo de memória física, tal qual o dado obtido venha como um despejo hexadecimal de forma bruta, no qual poderá ser analisado posteriormente a fim de obter informações legíveis que se julguem necessárias.

Neste método de extração por ser de alta complexibilidade, tem-se a vantagem na possibilidade da aquisição de arquivos apagados do sistema, sendo que pela extração lógica, isto poderia passar por despercebido. Entretanto, existe sua desvantagem, esta prática demanda de tempo e requer decodificação (MOSHE, 2012).

> "uma cópia bit a bit da memória flash física inteira usando o acesso de baixo nível. Desta forma, o sistema de arquivo não só do telefone é extraído, mas também o seu firmware e, mais importante, todos os dados não alocados." (MOOIJ, 2010)

Vale ressaltar, que a Memória Flash foi desenvolvida a partir de uma EEPROM (*Electrically-Erasable Programmable Read-Only Memory*), ou Memória Somente para Leitura Programável e Apagável Eletronicamente é uma memória não volátil, ou seja suas informações ainda serão armazenadas mesmo sem a presença de uma fonte de energia. No caso de uma varredura para extração de dados em um dispositivo móvel, a ferramenta fará uma aquisição diretamente na Memória Flash do mesmo. A figura abaixo demonstrará a exemplificação do funcionamento da extração física.

Figura 1. Organograma processual da extração física

Fonte: Elaborado pelos autores.

2.2.3. Extração Manual

Este método é considerado como um meio de último recurso e não muito recomendado, visto que, depende do trabalho manual propriamente dito do perito encarregado, e como citado anteriormente, poderá ocasionar perdas ou possíveis danos à evidência, o que de fato acarretará em conclusões imprecisas e de caráter pobre em obtenção de provas.

Nesta fase de extração, o usuário em questão, extrairá as informações através do acesso no sistema operacional e então de maneira seletiva, far-se-á a aquisição de evidências que sejam consideradas relevantes ao fato a ser julgado. É um processo bastante laborioso que exige paciência e tempo, portanto, é utilizado somente como último recurso disponível.

2.3. Ferramentas Utilizadas

Na computação forense, inúmeros são os dispositivos, técnicas, recursos e ferramentas utilizadas para a extração de evidências, seja em soluções de Software ou Hardware. Exemplos como XRY, Cellebrite UFED, Solo4 e a linha de *writeblocker* Tableau estão entre os mais famosos dispositivos utilizados no ramo forense computacional.

2.3.1. Micro Systemation XRY

Desenvolvido a partir de 2003 pela empresa sueca Micro Systemation, o XRY é um software designado à extração forense de dados de dispositivos móveis como Celulares, Smartphones, Tablets e também sistemas de navegação por GPS.

> "O sistema XRY é a primeira escolha entre as agências de aplicação da lei em todo o mundo, e representa um sistema forense móvel completo fornecido com todo o

equipamento necessário que você precisa para realizar um exame forense de um dispositivo móvel” (MICRO SYSTEMATION, 2014)

Dispõe de algumas versões, tais como as seguintes:

2.3.1.1. Logical

Como uma versão mais simples, o XRY Logical é a solução baseada em software para qualquer PC com plataforma Windows. Nesta versão, ele dispõe do hardware necessário para a realização de perícias em dispositivos móveis, sendo então própria para a realização de uma extração lógica de dados.

2.3.1.2. Physical

O XRY Physical, é a solução baseada na obtenção forense de dados apagados ou protegidos, sendo assim, obtidos pela extração física dos dados do dispositivo.

2.3.1.3. Complete

Consiste no kit contendo as funções Logical e Physical inclusas. Amplamente utilizado e recomendado na obtenção de evidências de dispositivos móveis, nesta versão, o usuário contará também com os dispositivos para clonagem de cartões do tipo SIM, uma unidade de comunicação e suas devidas ferramentas necessárias para uma extração física ou lógica, de maneira que o usuário obtenha uma extração de dados com o máximo de eficiência possível (Figura 2).

Figura 2. Exemplo do XRY Complete em pleno funcionamento. Nesta versão contém um case, kit de cabos, unidade de comunicação periférica, juntamente com a chave do dispositivo dentre outros acessórios.

Fonte: Micro Systemation

2.3.1.4. Field Version

Nesta versão do dispositivo (Figura 3), ela está adequada ao meio portátil de utilização imediata, sendo então de utilização em campo (do inglês *Field*, Campo). Segundo (MICRO SYSTEMATION, 2014), esta versão satisfaz algumas organizações, que frequentemente requisitavam kits forenses que fossem portáteis, ergonômicos e flexíveis, de tal forma que pudessem ser realizadas as perícias *in loco* e então pudessem facilmente conectar-se à sede ou em computadores remotos. Nesta versão acompanha o Panasonic CF-18, ou então intitulado

Toughbook, um computador bastante robusto, portátil e de alta autonomia de carga, que foi desenvolvido a partir do padrão militar MIL-STD-810F [4] para suportar condições extremas, tendo em vista que seu case seja composto por uma resistente liga de magnésio.

Figura 3. XRY Field Version. Versão portátil sendo também recurso para uso militar, estando incluso o Panasonic CF-18 Toughbook, kit de cabos, dentre outros acessórios.

Fonte: Micro Systemation

2.3.2. Cellebrite UFED

Desenvolvido a partir de 1999 pela empresa israelense Cellebrite Mobile Synchronization LTD, a série UFED ou Dispositivo Universal de Extração Forense, é atuante como um concorrente direto do Micro Systemation XRY. Amplamente utilizado pelas forças militares e também pelas agências de inteligência, é uma ferramenta importante para extração, decodificação e análise de dados de dispositivos móveis.

A série UFED possui também uma ampla variedade de versões, sendo as opções de campo *(TK - Turn Key)*, *Touch Logical*, *Touch Ultimate, 4PC Logical, 4PC Ultimate.*

2.3.2.1. Versões Touch

Segundo (CELLEBRITE, 2014), a versão *Touch* foi desenvolvida como um *standalone*, um dispositivo independente criado exclusivamente para a realização da extração forense de dispositivos móveis (Figura 4). O UFED *Touch* possui uma interface intuitiva, e sensível ao toque *(touchscreen)*, possibilitando também a realização de extração física (na versão *Ultimate*), lógica (na versão *Logical*), sistemas de arquivos e todos os tipos de dados e senhas, incluindo também arquivos apagados de uma ampla variedade de dispositivos móveis.

Além de ser uma versão portátil, o UFED *Touch* conta também com o kit operacional (cabos, conectores e etc).

Figura 4. Cellebrite Touch

Fonte: Cellebrite Mobile Synchronization

2.3.2.2. Versões 4PC

A versão 4PC foi desenvolvida como uma solução forense que funcione em um hardware existente, ou seja, num computador ou um notebook. Esta versão é versátil e conta com uma de aplicativos, acessórios e periféricos. Na versão *Ultimate*, conta com a possibilidade da realização de extração física (Figura 5).

Figura 5. Exemplo de funcionamento do Cellebrite 4PC

Fonte: Cellebrite Mobile Synchronization

2.3.2.3. Versão TK – Turn Key

Podendo ser considerada como a versão mais completa da série UFED, a versão *TK* ou *Turn Key*, foi desenvolvida para o uso recomendado em campo, fornecendo ao usuário todas as aplicações juntamente com todo o aparato necessário para a realização de análises forenses em condições adversas. Assim como, o XRY Field Version da empresa Micro Systemation, a versão *TK* além de contar também com a linha de laptops resistentes e robustos da Panasonic, a versão TK conta com o *Toughbook* CF-18 e CF-53, ou o *Toughpad* G1 (Figura 6).

Figura 6- Modelos do Cellebrite UFED, sendo este a versão TK.
À esquerda o Toughbook CF53, e à direita o Toughpad G1.

Fonte: Cellebrite Mobile Synchronization

2.3.3. Solo4

Desenvolvido pela empresa americana Intelligent Computer Solutions – ICS, o Image MASSter Solo4 é constituído de um hardware especialista em aquisição e duplicação em alta velocidade de dados de Discos Rígidos, amplamente utilizado no meio forense. A taxa de transferência e cópia de dados através deste dispositivo, correspondente a 13GB/min podendo alcançar incríveis 18GB/min, com suporte às interfaces SATA-2, IDE, SAS e USB.

A utilização deste equipamento, está relacionada a duplicação de dispositivos de grande quantidade de armazenamento, ou seja, HDs, ao qual poderá realizar a duplicação do Disco Rígido sem o auxílio de um computador, logo o SOLO-4 funciona como um dispositivo caracterizado como *standalone,* ou seja, poderá ser utilizado em campo. Todavia, o SOLO-4, também é capaz de realizar a sanitização de um disco rígido, o que segundo (ARANHA, 2013) resume-se em eliminar de maneira efetiva todos os dados de um disco.

Figura 7. Image MASSter Solo4 Forensic Superkit

Fonte: Intelligent Computer Solutions – ICS.

2.3.4. Tableau

No ambiente da computação forense, a empresa americana Guidance Software desenvolveu o dispositivo denominado "Tableau" funcionando como Duplicador e *Write Blocker*, mas segue a pergunta: O que é um *Write Blocker*?

> "As *forensics bridges* (bloqueadores de escrita) são fundamentais em qualquer kit de computação forense. Os examinadores têm em mãos uma tecnologia de alta velocidade capaz de gerar imagem dos atuais discos rígidos – grandes e velozes –, tanto em ambiente de laboratório quanto em campo." (FORENSE DIGITAL, 2014)

As *bridges* forenses, conhecidas como *Write Blockers*, consistem em ferramentas que realizem a imagem forense da evidência tendo somente o acesso à função *Read-Only*, ou seja, que tenha acesso apenas à leitura de um dispositivo de armazenamento sem comprometer a integridade da evidência, protegendo seus dados. Esta ferramenta está ligada diretamente ao fundamento principal da computação forense, baseada na máxima preservação dos dados em cadeia de custódia.

---

3. Metodologia

Em termos metodológicos para a realização da pesquisa, em relação aos objetivos, tratou-se de uma pesquisa descritiva e explicativa, com abordagem qualitativa e baseada na pesquisa bibliográfica, documental e de campo.

Pesquisa descritiva, para Gil (2002) têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis.

---

4. Conclusão

Embora as discussões sobre a computação forense remonte a virada do milênio (POLLIT et al., 2000), (NIJ, 2001), no Brasil a regulamentação dos crimes cibernéticos somente ocorreu em 2011, quando foi editada a Lei nº a nº 12.737/2011. Com o acréscimo dos artigos 154-A e 154-B, o Código Penal passou-se a tipificar os crimes de Invasão de dispositivo informático, Interrupção ou perturbação de serviço telegráfico, dentre outros praticados contra os meios de comunicação de utilidade pública. Igualmente, a ampliação da redação dos artigos 266 e 298 da legislação penal em vigente.

Não obstante o retardamento da inovação do aparato jurídico pátrio, a computação forense na definição que se entende mais adequada, revela que há uma gama de exames técnicos (perícias) cuja redução de dados e análise das evidências são passíveis do emprego de ferramentas equipadas com software e hardware de última geração. Igualmente, que a adoção de tais recursos não se restringe a investigação dos crimes cibernéticos, podendo também ser determinante na apuração de crimes organizados, como tráfego de drogas e lavagem de dinheiro, que em um dado momento podem valer-se da comunicação telefônica ou internet para a consumação dos delitos.

Diferente de outras espécies, as evidências digitais, tais como aquelas armazenas em discos rígidos de computadores em geral e smartphones, apresentam certo de grau de fragilidade, exigindo extremo cuidado na fase de extração. Para evitar a perda destas informações, pode-se verificar que a inovação tecnológica no campo da computação forense avançou significativamente na última década, a exemplo do aperfeiçoamento do *Cellebrite UFED* desenvolvido pela primeira vez no ano de 1999.

Notadamente, a transmissão de dados proveniente dos recursos de telecomunicação que já eram considerados serviços essenciais à luz da Constituição do Brasil, ganhou relevância dentre os crimes cibernéticos. Isso porque, a sociedade está incorporando cada vez mais às atividades do cotidiano a utilidade e comodidade dos recursos oriundos da Tecnologia da Informação e Comunicação (TICs). Enquanto que novos crimes podem surgir no meio cibernético, aqueles já

conhecidos pela criminalística adaptam-se facilmente ao novo cenário, que põe fim nas fronteiras existente entre as distintas gerações e grupos sociais. Por conseguinte, a solução dos crimes oriundos ou hospedeiros do ambiente virtual e eletrônico exige cada vez mais a atenção das autoridades de segurança pública, em especial o aperfeiçoamento da inteligência policial qual passa necessariamente pela adoção de equipamentos de ponta, como os que foram analisados nesta oportunidade.

Referências bibliográficas

ARANHA, Osvaldo. **Queira o Sr. Perito explicar como sanitizar HD's (wipe) com ENCASE 6.** 2013. Disponível em: <http://qperito.com/2013/11/29/queira-o-sr-perito-explicar-como-sanitizar-hds-wipe-com-encase-6/>. Acesso em: 06 maio 2015.

BEN-MOSHE, Yuval. Challenges in Physical Extraction of Modern Smartphones and Advance Methods to overcome. In: SANS DIGITAL FORENSICS SUMMIT, 8., 2012, Praga. **Cúpula.** Praga: Sans Digital Forensics, 2012. p. 7 - 15. Disponível em: <https://digital-forensics.sans.org/summit-archives/2012/Yuval-Ben-Moshe-challenges-with-physical-extraction-of-modern-smartphones-and-advanced-methods-to-overcome-them.pdf>. Acesso em: 23 mar. 2015.

BRASIL. Decreto nº 12737, de 30 de novembro de 2012. T**ipificação Criminal de Delitos Informáticos**. Brasilia, DF, 30 nov. 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 14 mar. 2015.

BRASIL. **Sistema Nacional de Políticas Públicas Sobre Drogas - Sisnad**. Brasilia, DF, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm>. Acesso em: 20 mar. 2015.

CELLEBRITE. **Sobre a Cellebrite.** Disponível em: <http://lang.cellebrite.com/pt/corporate/about-cellebrite>. Acesso em: 17 abr. 2015.

CELLEBRITE. **UFED 4PC Logical:** A solução forense movel baseada em software. Disponível em: <http://lang.cellebrite.com/pt/mobile-forensics/products/pc-based/ufed-4pc-logical>. Acesso em: 17 abr. 2015.

CELLEBRITE. **UFED 4PC Ultimate:** A solução forense movel baseada em software. Disponível em: <http://lang.cellebrite.com/pt/mobile-forensics/products/pc-based/ufed-4pc-ultimate>. Acesso em: 18 abr. 2015.

CELLEBRITE. **UFED TK:** O kit tático de análise forense móvel para condições difíceis. Disponível em: <http://lang.cellebrite.com/pt/mobile-forensics/products/turn-key/ufed-tk>. Acesso em: 17 abr. 2015.

CELLEBRITE. **UFED Touch Logical:** Análise forense móvel para linha de frente. Disponível em: <http://lang.cellebrite.com/pt/mobile-forensics/products/standalone/ufed-touch-logical>. Acesso em: 18 abr. 2015.

CELLEBRITE. **UFED Touch Ultimate:** Solução móvel forense completa. Disponível em: <http://lang.cellebrite.com/pt/mobile-forensics/products/standalone/ufed-touch-ultimate>. Acesso em: 17 abr. 2015.

ELECTRONIC CRIME SCENE INVESTIGATION: A Guide For First Responders. Washington, Dc: National Institute Of Justice, 2001. Disponível em: <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>. Acesso em: 20 mar. 2015.

ESPÍNDULA. Alberi. Perícia Criminal e Cível. Porto Alegre: Sagra Luzzatto. 2002. 343p.

EUA. Mark M. Pollitt. Fbi. Recovering and Examining Computer Forensic Evidence. **Forensic Science Communications.** [s.i], p. 1-7. out. 2000. Disponível em: <http://www.fbi.gov/about-us/lab/forensic-science-

communications/fsc/oct2000/index.htm/computer.htm>. Acesso em: 15 mar. 2015.

FIORILLO, Salvatore. Theory and practice of flash memory mobile forensics. In: PROCEEDINGS OF THE 7 TH AUSTRALIAN DIGITAL FORENSICS CONFERENCE, 7., 2009, [s.i]. **Conferência.** [s.i]: Proceedings Of The 7 Th Australian Digital Forensics Conference, 2009. p. 11 - 14. Disponível em: <http://www.theosecurity.com/pdf/Fiorillo.pdf>. Acesso em: 19 abr. 2015.

FORENSE DIGITAL. **Image MASSter SOLO-4:** Tecnologia avançada para cópia de HD. Disponível em: <http://www.forensedigital.com.br/wp-content/uploads/2014/07/Solo4.pdf>. Acesso em: 15 abr. 2015.

FORENSE DIGITAL. **Tableau - Utilidades e acessórios.** Disponível em: <http://forensedigital.com.br/product/tableau-utilidades-e-acessorios/>. Acesso em: 01 maio 2015.

FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT. Washington, Dc: National Institute Of Justice, 2004. Disponível em: <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>. Acesso em: 19 abr. 2015.

FRANÇA, Genival Veloso de. **Fundamentos da Medicina Legal.** [s.i]: Guanabara Koogan, 2005.

GIL, Antônio Carlos. Como Elaborar Projetos de Pesquisa. 5 ed.. São Paulo: Atlas, 2002.

ICS. **IM Solo-4 Forensic Super Kit:** Hard Drive Data Acquisition kit. Disponível em: <http://www.ics-iq.com/ImageMASSter-Solo-4-Forensic-Hard-Drive-Duplicator-p/f.gr-0043-000a.htm>. Acesso em: 22 mar. 2015.

INTELLIGENT COMPUTER SOLUTIONS. **Image MASSter SOLO-4 Forensics:** High Speed Forensic Acquisition & Data Sanitization. Disponível em: <http://www.ics-iq.com/v/vspfiles/files/datasheets/Solo-4 Forensic Brochure 1-2011.pdf>. Acesso em: 18 abr. 2015.

MOOIJ, Bram. **Data Extraction from a Physical Dump.** Disponível em: <http://www.forensicmag.com/articles/2010/09/data-extraction-physical-dump>. Acesso em: 21 mar. 2015.

MORIMOTO, Carlos E.. **Memória Flash.** Disponível em: <http://www.hardware.com.br/tutoriais/memoria-flash/>. Acesso em: 28 mar. 2015.

MSAB. **What is XRY?** Disponível em: <https://www.msab.com/xry/what-is-xry>. Acesso em: 20 mar. 2015.

MSAB. **XRY Field Version.** Disponível em: <https://www.msab.com/products/field-version/>. Acesso em: 20 abr. 2015.

MURPHY, Cynthia A.. **1 Developing Process for Mobile Device Forensics.** Disponível em: <http://www.mobileforensicscentral.com/mfc/documents/Mobile Device Forensic Process v3.0.pdf>. Acesso em: 01 abr. 2015

OPILHAR, Maria Carolina Milani Caldas. **Criminalística e Investigação Criminal.** Palhoça: Unisulvirtual, 2006. Disponível em: <http://busca.unisul.br/pdf/88717_Maria.pdf>. Acesso em: 01 maio 2015.

PANASONIC. **Padrões militares (MIL-STD).** Disponível em: <http://www.panasonictoughbook.com.br/porque-toughbook-alem-especificacoes-militares.asp>. Acesso em: 25 mar. 2015.

SONNTAG, Michael. **Introduction to Computer Forensics.** Disponível em: <https://www.sonntag.cc/teaching/Computer_Forensics_SS08/1-ComputerForensics/IntroductionToComputerForensics.pdf>. Acesso em: 01 mar. 2015.

WRITE Blockers. Disponível em: <http://www.cru-inc.com/data-protection-topics/write-blockers/>. Acesso em: 02 maio 2015.

1. Bacharel em Ciências da Computação pelo Centro Universitário Unifacvest e Pós-graduando em Computação Forense e Perícia Digital pelo Instituto de Pós-Graduação e Graduação - IPOG.

2. Bacharel em Direito pela Universidade do Planalto Catarinense (Uniplac) e mestrando em Desenvolvimento Regional da Universidade Regional do Noroeste do Rio Grande do Sul (Unijui).

3. Bacharel em Direito pela Universidade Regional do Noroeste do Rio Grande do Sul (Unijui) e mestrando em Desenvolvimento Regional da Universidade Regional do Noroeste do Rio Grande do Sul (Unijui).

4. O MIL-STD-810 é um padrão militar aprovado pelo departamento de defesa dos Estados Unidos da América (DoD). Este padrão enfatiza e estabelece, a produção e o design de equipamentos que suportem condições extremas ao longo de sua vida útil de funcionamento.

Revista ESPACIOS. ISSN 0798 1015
Vol. 38 (Nº 51) Año 2017

[Índice]