Universidade de Brasília
Faculdade de Direito

DO VALOR PROBATÓRIO DO ARQUIVO DIGITAL

Mônica Gomes Ramos

Trabalho de conclusão do curso apresentado como requisito parcial à obtenção do grau de Bacharel em Direito, da Faculdade de Direito da Universidade de Brasília. Área de concentração: Direito Processual Penal. Forense Digital.

Orientador:
Prof. Dr. Davi Monteiro Diniz

Brasília
2011

Monografia apresentada à Faculdade de Direito da Universidade de Brasília como requisito parcial para obtenção do grau de Bacharel.

Aprovado pela Banca Examinadora em 15 de Julho de 2011:

Banca Examinadora:

Prof. Dr. Davi Monteiro Diniz

Prof. Dr. Argemiro Cardoso Moreira Martins

Prof. Ms. João José Costa Gondim

RAMOS, Mônica Gomes.

Do valor probatório de arquivos digitais / Mônica Gomes Ramos – Brasília: UnB, Faculdade de Direito, 2011.

p. 82: il.

Monografia – Universidade de Brasília, Faculdade de Direito, Brasília, 2011.

Orientador: Diniz, Davi Monteiro.

Documento eletrônico, Valor Probatório, Arquivo Digital, Processo Penal, Processo Criminal.

Dedico esse trabalho ao meu esposo, Carlos Bimbato, que soube respeitar como ninguém as minhas ausências, e aos meus filhos, Ângelo e Amanda, que foram minha constante fonte de inspiração. A eles, que o meu esforço sirva de exemplo.

"Sonhar mais um sonho impossível,
Lutar quando é fácil ceder,
Vencer o inimigo invencível, (...),
Voar num limite improvável,
Tocar o inacessível chão,
É minha lei, é minha questão."
Chico Buarque

AGRADECIMENTOS

Há muitos anos entrei na UnB. Aqui tive um longo e árduo caminho. Iniciei pela Computação, adentrei à Ciência da Informação e agora encerro mais uma etapa no Direito.

Muitos anos passei nessa querida Universidade e é a ela que devo todo meu carinho e respeito.
Aqui me tornei o que sou. E por tudo que aprendi e pelo que consegui realizar, o meu muito obrigada.

Gostaria de agradecer também ao colega Alexandre que me indicou o meu orientador. Uma feliz escolha.

O Prof. Davi Diniz soube me orientar com maestria e com muito carinho. Graças a suas ponderações, consegui realizar um trabalho do qual me orgulho. A ele, meu sincero reconhecimento.

Também gostaria de agradecer ao Prof. João Gondim que me tirou várias dúvidas ao longo desse trabalho.

Por fim, não poderia deixar de agradecer a minha família, ao meu pai, a minha irmã, e em especial, a minha mãe, que sofreu comigo por cada noite mal dormida ao longo desses infindáveis anos.

Mãezinha, agora vou descansar um pouco. Só não sei até quando...

Sumário

RESUMO

O substancial aumento da capacidade de processamento dos computadores modernos e a adesão maciça dos usuários às redes mundiais provocaram uma grande revolução na sociedade atual. As informações que antes eram apresentadas somente em papel passaram a ser geradas de forma digital. Nesse contexto, uma importante reflexão a ser feita refere-se à utilização de arquivos digitais como prova em juízo.

Um dos grandes problemas para se admitir o arquivo digital como meio de prova era a impossibilidade de determinar a autoria e a autenticidade devido à ausência de uma assinatura manuscrita. Contudo, com a promulgação da Medida Provisória 2200-2/01, que instituiu a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), os documentos eletrônicos com assinatura digital passaram a ser aceitos como prova e essa discussão foi superada.

Cabe perguntar, contudo, o que fazer com a grande quantidade de arquivos digitais que não utilizam a assinatura digital para atestar a sua autoria? Como atestar a autenticidade e a integridade desses arquivos que correspondem a mais de noventa por cento dos documentos gerados atualmente, sem comprometer o devido processo legal? Como garantir que esses documentos não tenham sido violados ou que não sejam provas plantadas? Como essas novas tecnologias podem nos auxiliar a responder essas perguntas?

Sem o objetivo de exaurir a discussão, esse trabalho tem como objetivo fazer uma reflexão sobre os instrumentos utilizados pela forense digital para atestar a autoria e a integridade dos arquivos digitais, e garantir, portanto, seu uso como prova em processos, em especial, processos criminais que são ainda mais restritivos quando se trata de matéria de prova.

INTRODUÇÃO

A disseminação das novas tecnologias, a popularização dos computadores e a expansão do uso da Internet geram impactos comportamentais, éticos e legais. Para Pinheiro, "as principais mudanças consistem na virtualização das relações, onde a manifestação de vontade passa cada vez mais a ser não presencial, as testemunhas passam a ser máquinas e o documento original passa a ser o digital, o formato impresso é mera cópia".[1]

O papel foi a primeira forma de virtualizar as relações humanas, uma vez que, antes de sua existência, a maioria dos atos geradores de direitos e obrigações eram praticados de forma presencial, oralmente ou na presença de testemunhas. Hoje, vemos cada vez mais as relações humanas serem consolidadas por meio de novas tecnologias.

Assim, para que o Direito continue a cumprir seu papel na harmonização e garantia da segurança das relações sociais, torna-se imperativo sua adequação aos novos paradigmas sociais. O Direito não baseado na realidade está obsoleto e não preserva a qualidade de sua eficácia jurídica[2].

A forma como as pessoas se relacionam, se obrigam, e a própria forma de provar tudo isso está sendo modificada pelas novas tecnologias[3]. O substancial aumento de processamento dos computadores modernos, a adesão maciça dos usuários às redes mundiais e a expansão da comunicação sem fio em banda larga provocaram uma grande revolução na sociedade atual, e isso, por sua vez, demanda uma adaptação dos conceitos jurídicos.

Nesse cenário, uma importante reflexão a ser feita refere-se à utilização de arquivos digitais como prova em juízo. Os arquivos eletrônicos não podem ser dissociados do meio físico em que se encontram e dependem do computador para serem acessados. Contudo, essas características em nada diminuem sua importância, quando se trata de sua força probatória. Ademais, no que se refere aos processos criminais, a prova assume uma relevância ainda maior, uma vez que é por meio dela que se busca a verdade manifesta dos fatos, que podem ou não levar à imposição de restrições à liberdade.

É certo que, quando se trata de documento em papel, a nossa legislação já está plenamente adaptada, haja vista que o meio jurídico se fundamenta nesse suporte para

---

[1] PINHEIRO, 2006, p. 9.
[2] Idem , 2006, p. 10.

legitimar suas transações. Nas últimas décadas, contudo, percebe-se a ansiedade em mostrar que documento e documento eletrônico independem do suporte material e, por isso, as leis podem ser aplicadas da mesma forma, apenas com uma leve mudança na ótica jurídica.

A impossibilidade de determinar a autoria e a autenticidade devido à ausência de uma assinatura manuscrita era um dos grandes problemas para se admitir o arquivo eletrônico como meio de prova[4]. Contudo, com a crescente utilização dos recursos tecnológicos, a assinatura manuscrita, caracterizada pela oposição do nome no documento, está sendo substituída pela utilização de senhas, haja vista a ampla utilização do cartão de crédito em transações bancárias e em negócios realizados no comércio eletrônico. Essa mudança representa uma adaptação a uma nova realidade social.

Ademais, com a promulgação da Medida Provisória 2200-2/01, que instituiu a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), essa discussão foi superada. Os documentos eletrônicos que utilizam a assinatura digital para garantir sua autenticidade e sua integridade já são amplamente aceitos como prova pelo judiciário brasileiro.

Cabe perguntar, contudo, o que fazer com a grande quantidade de arquivos digitais que não possuem assinatura digital? Os documentos eletrônicos gerados pelos serviços de home banking, as informações comprobatórias de desvio de fluxo de caixa extraídas de computadores apreendidos pelos fiscais da Receita Federal, o material pornográfico infantil rastreado e fornecido pelos provedores de acesso são exemplos de arquivos que não possuem certificação digital. Contudo, ninguém poderia negar a sua força probatória e, por isso, esses deveriam integrar as provas responsáveis por formar a convicção do juiz.

No último dia 02 de Maio, foram apreendidos vários HDs, CDs, DVDs e drives USB nas instalações do então líder da Al Qaeda, quando Bin Laden foi morto por uma elite militar norte-americana. Nas palavras de Richard Haass, conselheiro para negócios estrangeiros e ex-presidente do Departamento de Estado americano, a “apreensão da inteligência pode ser tão importante, se não mais importante, que a morte real de Bin Laden.” [5] Essas informações, que estão sendo processadas e analisadas, serão utilizadas em um esforço

---

[3] PINHEIRO, 2006, p. 13.
[4] GICO JUNIOR ,2000a., p. 350.
[5] NOBREGA , 2011.

conjunto contra o terrorismo e poderão ser usadas para fundamentar acusações em possíveis processos criminais.

Diante do exposto, vários questionamentos podem ser feitos. É possível usar esses arquivos como prova? Se a autoria é um aspecto fundamental na prova documental, como garantir a autoria de documentos que se encontram em meio magnético? É certo que a criptografia e a assinatura digital vêm como resposta à autoria de documentos digitais. Mas, é bem verdade, que a maioria dos documentos gerados atualmente não utiliza nenhum desses mecanismos. Ainda sim, é possível usá-los como meio de prova?

Como atestar a autenticidade e integridade desses arquivos que correspondem a mais de noventa por cento dos documentos gerados atualmente, sem comprometer o devido processo legal? Como garantir que esses documentos não tenham sido violados ou não sejam provas plantadas? Como essas novas tecnologias podem nos auxiliar a responder a essas perguntas?

A grande revolução computacional provocou uma mudança de costumes e está cada vez mais sendo utilizada na realização de atividades ilícitas. Além de serem utilizados como ferramentas na consumação de certos crimes, os computadores podem conter evidências preciosas relacionadas a essas atividades[6] [7].

Qualquer informação armazenada ou transmitida em formato digital, seja dado ou software, pode ser uma evidência, se ele tem significado relevante para a investigação. Cabe ressaltar que as informações existem por serem úteis a alguma atividade humana. Assim, entender como obter e utilizar essas evidências nos leva a estudar conceitos da forense digital, que envolve aquisição, preservação, identificação, extração, restauração, análise e documentação de evidências computacionais.

Nesse sentido, a ciência forense digital vem como resposta a essa inquietude e será objeto de reflexão da presente pesquisa. Sem o objetivo de exaurir a discussão, esse trabalho tem como objetivo fazer uma reflexão sobre os instrumentos utilizados pela perícia digital para atestar a autoria e a integridade dos arquivos digitais, e garantir, portanto, seu uso como prova em processos, em especial, processos criminais que são ainda mais restritivos quando se trata de matéria de prova.

---

[6] REIS & GEUS, 2010, p. 58.
[7] Idem , 2001, p. 37.

É possível, portanto, demonstrar a autoria e a autenticidade dos arquivos digitais criptografados, e mesmo aqueles que não utilizem mecanismos de criptografia ou assinatura digital são aptos a serem utilizados como prova em processos, desde que cumpram determinados requisitos técnicos definidos pela perícia.

Assim, esse documento será composto por dois capítulos. No primeiro serão apresentados os fundamentos dessa pesquisa, com uma exposição dos conceitos a serem utilizados. No outro capítulo, parte essencial do trabalho, faremos uma apresentação da perícia forense aplicada à informática, demonstrando a importância de seguir determinados procedimentos no processo de análise de arquivos digitais com o fito de garantir seu valor probatório em processos judiciais. Por fim, as conclusões serão apresentadas ao término do trabalho.

CAPÍTULO I – FUNDAMENTOS

O presente capítulo tem como objetivo apresentar os conceitos relacionados a prova e dados, assuntos que serão considerados no estudo do uso de arquivos digitais como prova nos processos, sejam cíveis ou criminais.

1) Prova

O sistema de prova legal varia conforme os diferentes ordenamentos jurídicos. Assim, os preceitos que norteiam o legislador para definir as regras de prova dependem do interesse da sociedade, da proteção às liberdades individuais e civis, e, principalmente, da necessidade de nunca se castigar um inocente. Por outro lado, um delito sem punição é um estímulo a ocorrência de mais crimes. Nesse sentido, a única forma de coibir a ocorrência de delitos é garantir ao criminoso a aplicação de pena justa e na medida de seu delito Assim, com o objetivo de impedir uma condenação injusta, há que se analisar criteriosamente todas as provas apresentadas.

Uma sentença deve revelar se o crime foi cometido, se foi feito pelo acusado, e, as circunstâncias de sua execução[8]. A verdade dos fatos apresentada na sentença fundamenta-se nas provas. Em matéria criminal, é sobre as provas que recaem as prescrições legais mais importantes.

Em uma comparação entre o processo criminal e o civil, pode-se afirmar que há um conjunto de princípios comuns que decorrem da mesma natureza do processo em geral, o que se busca em ambos é sempre a "manifestação da verdade" [9]. Contudo, no processo criminal, o interesse público é o responsável pelo procedimento e a parte não tem o condão de fazê-lo parar.

Além disso, a aplicação da sanção depende da comprovação dos fatos ofensivos denunciados e requer uma intervenção *ex officio* do inquiridor criminal. Ou seja, em esfera criminal, o papel do inquiridor se alarga, uma vez que se preocupa "por chegar à verificação

[8] MITTERMAIER, 1997, p. 58.

do delito, ao reconhecimento do seu autor e à demonstração clara e perfeita de todos os detalhes, de que pode depender a aplicação justa da pena" [10].

A prova no processo criminal assume uma relevância muito maior, uma vez que é por meio dela que se busca a verdade manifesta dos fatos, que podem ou não levar à imposição de restrições à liberdade. Quatro consequências decorrem dessa assertiva: em primeiro lugar, o círculo das provas torna-se mais restrito no processo criminal do que nos demais processos; a confissão só motiva uma condenação se o juiz tiver certeza absoluta da autoria do crime; em matéria criminal, a desistência do acusado não tem influência no processo; por fim, as prescrições legais admitidas no processo cível não valem para o processo criminal, tais como dilações peremptórias, força da coisa julgada e revelia não acarretam condenação.

É considerada uma base de argumentação para formar a convicção do juiz e utilizada para "patentear a evidência dos fatos". Sabe-se que nos processos criminais, os autores dos delitos têm como objetivo eliminar todos os vestígios, buscando, assim, comprometer a convicção do juiz.

É consenso definir prova como "No sentido legal, os meios de prova, ou, em uma palavra, as provas, são para o juiz as fontes dos motivos de convicção que a lei declara suficientes para, aplicados aos fatos da causa, determinarem naturalmente a sentença" [11].

Assim, "provar é querer, em substância, demonstrar a verdade e convencer o juiz, o qual para decidir há mister de adquirir plena certeza" [12]. E continua, "Todo o meio de produzir a certeza será necessariamente um meio de prova".[13]

Entende-se ainda como prova como "tudo aquilo que é capaz de demonstrar a veracidade ou autenticidade de algo. Não se fala em prova senão a respeito de algo que venha afirmado, para provar-lhe exatidão. Na ciência é tudo aquilo que dá base de sustentação a uma dada afirmação científica e que pode ser repetida por qualquer outro cientista, para que alcance o mesmo resultado afirmado, desde que realizado nos mesmos termos" [14].

---

[9] MITTERMAIER, 1997, p. 65.
[10] Idem, p.70.
[11] Idem , p. 149.
[12] Idem , p. 79.
[13] Idem , p. 146.
[14] GICO JUNIOR , 2000c, p. 305.

No Direito, o termo também é plurissignificativo abrangendo tanto a atividade procedimental, quanto o resultado desta atividade. Assim, para bem compreender seu significado, há que se estudar prova, meio de prova, motivo de prova e produção da prova.

A prova tem como objetivo gerar no juiz a convicção de que necessita para o seu pronunciamento, assim, representa "um conjunto de atos praticados pelas partes, por terceiros (testemunhas, peritos, etc.) e até pelo juiz para averiguar a verdade e formar a convicção deste último" [15].

Assim, a prova refere-se ao ato de convencer outra pessoa quanto à verdade dos fatos e o meio de prova ao instrumento utilizado na produção da prova, com o objetivo de produzir a convicção do juiz[16].

Provar, portanto, é o ato de demonstrar a alguém a veracidade ou verossimilhança de uma dada alegação. O ***objeto da prova*** refere-se ao que se deve demonstrar, isto é, abrange não só o fato criminoso e sua autoria, como todas as circunstâncias objetivas e subjetivas que possam influir na responsabilidade penal e na fixação da pena. Quanto ao objeto, a prova pode ser ***direta*** quando por si demonstra o fato, ou ***indireta*** quando se permite concluir o alegado a partir da comprovação de um outro fato.O ***meio de prova*** é a forma pela qual a alegação e as representações são apresentadas e podem ser: documentos, testemunhos, instrumentos apresentados, vistorias, etc. Uma vez que no processo penal brasileiro vigora o princípio da verdade real, não há nenhuma limitação aos meios de prova.

A ***produção da prova***, por sua vez, refere-se ao ato de "trazer em juízo a prova pré-constituída ou de efetivamente produzir o elemento que integrará o processo como prova". Por fim, ***motivo de prova*** "é toda e qualquer alegação contestada por uma das partes ou que não está satisfatoriamente clara no processo na visão do juiz. Refere-se aos fatos pertinentes ao processo, os fatos jurídicos relevantes e as alegações deles decorrentes, que devem ser idoneamente provadas" [17] .

Os meios de provas podem ser assim classificados:

a) Inspeção e verificação judicial – Resultam da observação do juiz;

b) Prova por perito – utilizando sua competência técnica, os peritos fazem um exame e apresentam relatório com suas conclusões;

---

[15] MIRABETE ,2006, p. 247.
[16] GICO JUNIOR ,2000c, p. 306.
[17] Idem ,2000c, p. 305.

c) Confissão do acusado – reconhecimento realizado em juízo, por uma das partes, a respeito da veracidade dos fatos que lhe são atribuídos e capazes de ocasionar-lhe conseqüências jurídicas desfavoráveis;
d) Prova testemunhal – oitiva de pessoas, perante o juiz, que declaram o que sabem acerca dos fatos sobre os quais se litiga no processo penal;
e) Indícios – circunstâncias conhecidas e provas que, tendo relação com o fato, autorizem, por indução, concluir-se a existência de outra ou outras circunstâncias;
f) Peças de convicção e documentos – ainda que por si só não representem a materialidade do crime por serem provas secundárias, podem ser considerados meios de prova quando associados à confissão ou à prova testemunhal.

Ainda que considere a seguinte divisão sem objetivo prático, Mittermaier[18] afirma que a prova imediata leva diretamente à convicção, enquanto a prova circunstancial só é concludente por meio das induções. A prova natural, por sua vez, relaciona-se à evidência material e a prova artificial baseia-se nos indícios.

Com o objetivo de formar a sua convicção, o juiz aprecia os diversos meios que se contrapõem à causa[19], Nesse sentido, para que possa haver a decretação da pena, a prova de acusação deve ser inteira e completa. Assim são objetivos da prova de acusação:
a) Verificação da existência de todos os fatos que levam à materialidade do ato criminoso;
b) Demonstração de o acusado ter participado do crime culpadamente;
c) Exame do estado mental do acusado e de sua vontade de realizar o crime;
d) Manifestação de premeditação;
e) Indagação da intencionalidade;
f) Demonstração da relação direta entre a intenção e os fatos criminosos ou da imputabilidade.

Para admitir a acusação, o juiz deve exigir que seja demonstrada sua veracidade. Além disso, bastará apenas uma dúvida quanto à culpabilidade, para que a condenação seja impedida. Rege o princípio *in dúbio pro réu* que todo caso duvidoso seja interpretado a favor do acusado. Nesse sentido, não há como transportar o mecanismo das exceções do processo

[18] MITTERMAIER, 2007, p. 153
[19] Idem, p. 164.

civil para o processo criminal, incorrendo, nesse caso, em ataque frontal às amplas garantias instituídas pelos princípios constitucionais.

No âmbito criminal, não há como separar a prova da acusação da prova da defesa. Pelo contrário, todas as provas são analisadas com o objetivo precípuo de formar a convicção do juiz. Ao contrário do processo civil, basta que as alegações de defesa sejam verossímeis, para que uma sentença favorável seja proferida. A dúvida será interpretada sempre em favor do acusado e a verossimilhança de suas alegações influirá na medida da pena[20].

É possível que certos fatos nos processos criminais sejam provados por meios de documentos e de peças de convicção. Há entendimento pacífico de que todo documento poderá ser utilizado como prova desde que seja apresentado inteiro, completo, sem qualquer vestígio de alteração ou mutilação; e, respeite sua forma obrigatória, sob pena de nulidade[21].

A mesma distinção dos documentos feita no cível vale para os processos criminais, ou seja, os documentos podem ser públicos ou particulares. Os documentos públicos devem respeitar as formas exigidas por lei ou por normas oficiais. Já os documentos particulares que não atentarem às formas substanciais funcionam como provas testemunhais. Contudo, podem fazer prova contra o autor.[22] Para os documentos públicos, essa sinceridade é comprovada quando revestida de todas as formalidades exigidas, o que implica numa presunção jurídica de "sinceridade[23]".

Quanto aos documentos particulares, a sinceridade pode ser comprovada pelo reconhecimento do autor do documento perante o juiz, o que implica em confissão; pelo reconhecimento feito por testemunhas; ou, pelo exame de peritos em peças de comparação. Sempre que houver alguma dúvida quanto à "sinceridade" dos documentos, será possível a realização de exames por peritos. Demonstrada a sinceridade, há que se analisar seu conteúdo o que implicará no seu efeito no processo.

Os meios de prova permitidos em nossa legislação não se esgotam no Código de Processo Penal. A previsão legal é exemplificativa, sendo admitidas as provas não previstas expressamente na legislação. Por outro lado são inadmissíveis as provas que ferem os princípios de respeito ao direito de defesa e à dignidade humana, bem como as provas de

[20] MITTERMAIER, 1997, p. 174.
[21] Idem, p. 385.
[22] Idem , p. 395.
[23]MITTERMAIER conceitua sinceridade como "apresentação no estado exato e fiel em que saiu das mãos de seu autor" (p. 399).

invocação ao sobrenatural. Além disso, não são admitidas as provas que violarem as normas legais ou os princípios do ordenamento de natureza processual ou material.

As provas circunstanciais ou indiciárias têm o mesmo valor das provas diretas, uma vez que inexiste hierarquia de provas. Assim, indícios múltiplos e concatenados são suficientes para fundamentar uma decisão condenatória, desde que não haja nenhum indício isolado que leve a uma explicação diferente. Vale, portanto, o princípio da livre convicção ou da verdade real, onde cabe ao juiz formar sua convicção por meio da livre apreciação das provas apresentadas.

2) Admissibilidade do arquivo digital como prova

Intermináveis são os exemplos da utilização de arquivos digitais no dia-a-dia: recibo de pagamento, ingresso, inscrição para concurso público, dentre outros. Mesmo na esfera jurídica, o arquivo digital já é uma realidade, a citar o acompanhamento processual e a cópia impressa do julgado.

Determinada linha doutrinária defende que em breve período de tempo, toda a atividade de armazenamento de documentos será feita de forma digital e que o documento cartular perderá grande parte de seu uso e de sua importância para o documento eletrônico [24]. Com a devida data vênia, em decorrência principalmente de questões culturais e técnicas, ainda está longe de o papel deixar de ser utilizado como suporte documental. Contudo, isso não nega a importância e a expansão do uso do arquivo digital, o que nos leva a refletir sobre seu valor jurídico como prova em juízo.

Antes de avaliar a admissibilidade do arquivo digital como prova, far-se-á um breve retrospecto sobre os conceitos de documento, documento eletrônico e arquivo digital, para melhor compreender o objeto de estudo do presente trabalho.

Para a Ciência da Informação, área que tem como propósito estudar a informação registrada em qualquer suporte físico, de forma genérica, documento é assim definido:

[24] GICO JUNIOR ,2000c, p. 302.

> *"... o conjunto de todos os suportes físicos existentes (livros, filmes, fitas, K-7, vídeos, CDs, periódicos, anais de congressos, atas, relatórios, cartazes, manuscritos, fotografias, teses, histórias em quadrinhos, mapas, plantas) nos quais estão as informações produzidas pelo conhecimento humano." A ABNT define documento como "qualquer unidade, impressa ou não, que seja passível de catalogação ou indexação[25]".*

Arquivo digital é definido como:

> *"Um conjunto finito de dígitos ao qual se atribui um nome, sendo neutro quanto à representação do conteúdo do arquivo, que pode variar de acordo com a utilidade e a função eventualmente emprestada ao arquivo quando manuseado através de um computador" [26].*

Documento eletrônico, por sua vez, é "o arquivo eletrônico capaz de representar um fato através do tempo e do espaço" [27]. Assim, possibilita sua utilização simultânea em qualquer lugar do mundo. Pode ser divido em sentido lato e em sentido estrito. Em sentido lato, requer uma máquina para a compreensão de seu conteúdo. Nesse caso, incluem-se os documentos gerados pelos cartões magnéticos. Já os documentos em sentido estrito não demandam um intermediário eletrônico para sua compreensão, incluem-se aí os documentos digitalizados, ou seja, cópias digitais dos documentos cartulares originais.

Do ponto de vista jurídico, documento pode ser entendido como "todo e qualquer registro, que expresse um pensamento, capaz de influenciar a cognição do juízo acerca de um dado fato em um dado processo[28]". A prova documental é sempre uma prova real e o meio físico sobre o qual incide o registro não pode invalidar a natureza documental da prova. Logo, é claro que "o Direito positivo não exige que o documento tenha como suporte físico o papel".

Outra importante definição jurídica de documento é:

> *"1. Direito Civil. a) escrito oficial que identifica uma pessoa; b) instrumento escrito que, juridicamente, faz fé daquilo que atesta, tal como contrato, escritura pública, certificado, atestado, recibo, título etc.; 2. Direito Processual Civil e Direito Processual Penal. a) Qualquer escrito oferecido em juízo que forneça prova de alegação do litigante; b) qualquer fato que possa comprovar ou testemunhar algo".[29]*

---

[25] GALVÃO ,1998, p. 46.
[26] DINIZ ,1999, p.21.
[27] GICO JUNIOR , 2000c, p. 303.
[28] Idem , 2000c, p. 305.
[29] DINIZ , 2005, p. 25.

Documento pode, ainda, ser definido como “qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizá-la para extrair cognição do que está registrado” [30] . De forma mais estrita, “é a peça escrita ou gráfica que exprime algo de valor jurídico para esclarecer, instruir ou provar o que se alegou no processo pelas partes em lide” [31]. Não basta a manifestação de um pensamento, há que representar um fato.

Quanto à relação desses conceitos com informação, a pirâmide informacional proposta por Urdaneta[32] propõe uma hierarquia para diferenciar dado, informação, conhecimento e inteligência, baseada nos conceitos de qualidade e quantidade, ou seja, quanto mais próximo do ápice, mais próximo do conceito de qualidade, e quanto mais próximo da base, mais próximo da quantidade.

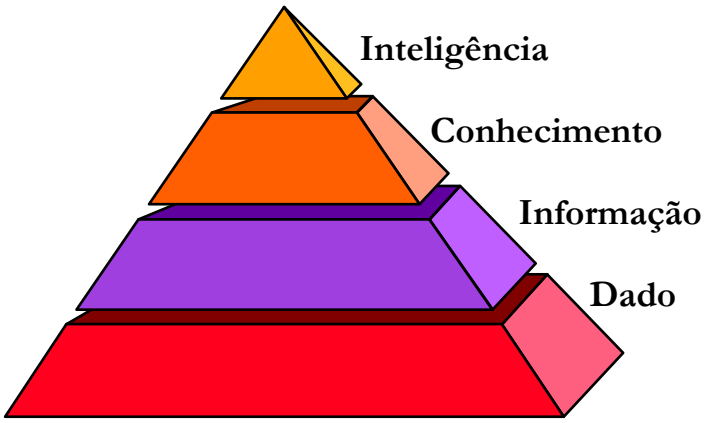


Figura 1 – Pirâmide Informacional (Urdaneta, 1992, p.100)

Ao falar de ***dados***, trata-se a informação como matéria e, nesse caso, o fator decisivo é a quantidade de dados. Ao tratar ***informação***, busca-se atribuir um significado ao dado. O importante nesse caso é o ordenamento desses a fim de obter um sentido cognitivo relevante. O estado informacional surge quando algo novo se contrapõe a algo que já seja conhecido.

Por sua vez, entende-se ***conhecimento*** como a compreensão da informação. Está relacionado com as estruturas informacionais que se integram aos sistemas de relacionamento simbólico de mais alto nível e permanência. Em verdade, acontece quando o receptor, ao

[30] GICO JUNIOR , 2000c, p. 305.
[31] Idem , p. 305.
[32] URDANETA ,1992, p.100.

perceber a informação, a internaliza, a contrapõe às experiências já vividas e então agrega valor ao já conhecido.

Por último, a ***inteligência*** é alcançada ao conceber a informação como oportunidade. Está ligada a possibilidade de mudar o *status quo* a partir das informações recebidas. Por isso, a qualidade dessas informações torna-se tão relevante.

Adotando essa pirâmide informacional, percebe-se que os arquivos digitais compõem as camadas mais inferiores, sejam elas, relacionadas a dados, de onde se pode extrair a informação. Mas, essas camadas são apenas o suporte informacional disponibilizado aos magistrados para que possam formar a sua convicção. Assim, a compreensão dessa informação compõe a estrutura informacional de mais alto nível responsável pelo resultado de seus julgados.

No âmbito legislativo, não faltam tentativas de adaptar os conceitos citados aos novos paradigmas[33] [34]. É certo que, quando se trata de documento em papel, a nossa legislação já está plenamente adaptada haja vista que o meio jurídico se fundamenta no documento para legitimar suas transações. Nas últimas décadas, contudo, percebe-se uma ansiedade muito grande em mostrar que documento e documento eletrônico não são conceitos diferentes, e que independem do suporte material e, por isso, as leis podem ser aplicadas da mesma forma, apenas com uma leve mudança na ótica jurídica.

Há inclusive legislação internacional que visa garantir a admissibilidade e a força probante dos documentos eletrônicos. Criada pela Assembléia Geral da Organização das Nações Unidas que instituiu uma lei modelo, a UNCITRAL defende em seu artigo 9º a admissibilidade e a força probante das mensagens de dados e dispõe que em procedimentos judiciais, administrativos ou arbitrais não haja norma jurídica que seja óbice à admissibilidade de mensagens eletrônicas como meio de prova[35].

---

[33] "*Projeto de Lei Nº 2644/96* - Considera-se documento eletrônico, para efeitos desta Lei, todo documento, público ou particular, originado por processamento eletrônico de dados e armazenamento em meio magnético, optomagnético, eletrônico ou similar."

[34] " *Projeto de Lei 4906/01* - Art. 2º Para os efeitos desta lei, considera-se: I – documento eletrônico: a informação gerada, enviada, recebida, armazenada ou comunicada por meios eletrônicos, ópticos, optoeletrônicos ou similares;"

[35] "Artigo 9º - Admissibilidade e força probante das mensagens de dados1) Em procedimentos judiciais, administrativos ou arbitrais não se aplicará nenhuma norma jurídica que seja óbice à admissibilidade de mensagens eletrônicas como meio de prova a) Pelo simples fato de serem mensagens eletrônicas; ou, b) Pela simples razão de não haverem sido apresentadas em sua forma original, sempre que tais mensagens sejam a melhor prova que se possa razoavelmente esperar da pessoa que as apresente.2) Toda informação apresentada sob a forma de mensagem eletrônica gozará da devida força probante. Na avaliação da força probante de uma mensagem eletrônica, dar-se-á atenção à confiabilidade da forma em que a mensagem haja sido gerada,

A linguagem eletrônica expressa a manifestação exterior da regulação dos interesses, ou seja, o computador não só aponta a vontade externa, bem como determina o conteúdo de tal vontade[36]. Assim, o arquivo digital residente na memória de um computador pode e deve ser utilizado pela parte interessada em um processo como forma de influir na cognição do juízo.

O documento como a prova e o suporte do documento como meio de prova são coisas distintas. Assim, "a forma de organização não é relevante desde que se obtenha a cognição[37]". Um documento não deve estar atrelado a um mero suporte, seja ele qual for. Ademais, "as provas no Direito Digital estão nas máquinas, pois estas é quem são as testemunhas[38]".

Quanto à autenticidade, além da facilidade de armazenamento, o documento eletrônico permite que a cópia do documento seja igual a do original eletrônico, em conformidade com o que pretendeu o autor. A inalterabilidade refere-se "a capacidade de determinar a inviolabilidade do arquivo eletrônico[39]". Tal característica está diretamente ligada à confiabilidade no conteúdo do documento o que implica na formação da convicção do juiz e sua livre apreciação das provas.

Essa confiabilidade se dá pela indicação da autoria o que, de forma geral, pode ser comprovada pela assinatura ou subscrição, do documento. Assim, a assinatura representa uma declaração de autoria do documento, bem como, reconhecimento de seu conteúdo. A assinatura pode tanto referir-se à oposição de um nome em um determinado documento, bem como à oposição de um símbolo.

Um dos grandes problemas em se admitir o documento eletrônico como meio de prova era a impossibilidade de se determinar a sua autoria e, portanto, a sua autenticidade, pelo fato de que neles não se opõe uma assinatura manuscrita[40]. Contudo, com a crescente utilização dos recursos tecnológicos, a assinatura manuscrita, caracterizada pela oposição do nome no documento, está sendo substituída pela utilização de senhas, vide a ampla utilização do cartão de crédito em transações bancárias e em negócios realizados no comércio

---

armazenada e transmitida, a confiabilidade da forma em que se haja conservado a integridade da informação, a forma pela qual se haja identificado o remetente e a qualquer outro fator pertinente."

[36] GICO JÚNIOR ,2000b, p. 320.

[37] Idem, p. 326.

[38] PINHEIRO ,2006, p. 13.

[39] GICO JÚNIOR,2000a, p. 326.

[40] Idem , 2000a, p. 350.

eletrônico. Essa mudança representa uma adaptação a uma nova realidade social que se apresenta.

Quanto à assinatura eletrônica, "é a marca ou informação capaz de identificar através de averiguação eletrônica[41]". Para tanto, podem ser usados senhas, conjunto de caracteres alfanuméricos conhecido apenas pelo usuário, ou biodados, tais como reconhecimento de íris, voz, altura ou mesmo o formato da face, que quando comparados aos dados contidos em bancos de dados, atestam ou não a autoria do documento eletrônico.

Para que um documento eletrônico tenha força probante, portanto, deve atender aos seguintes requisitos[42]:

a) ***Autenticidade*** – Processo pelo qual se pode garantir a autoria do documento eletrônico, ou seja, não permite dúvida quanto à identificação do autor.

b) ***Integridade*** – Permite atestar a "inteireza do documento eletrônico após sua transmissão, bem como apontar eventual alteração irregular de seu conteúdo".

A criptografia e a certificação digital são mecanismos já reconhecidos de garantia da autoria e da integridade de um documento eletrônico. Criptografia pode ser entendida como a técnica de escrever em cifra ou em código, cuja principal função é permitir que dois interlocutores se comuniquem privativamente, através de um canal público ou inseguro, de forma tal que um tenha certeza de quem é o outro[43]. Amplamente utilizada em assuntos de Estado, seu uso em transações comerciais já é uma realidade.

A **criptografia de chave pública** ou **criptografia assimétrica,** primeiro mecanismo a possibilitar encriptação e assinatura digital, é uma das grandes inovações em criptografia de chave pública. É um método de criptografia que utiliza um par de chaves: uma **chave pública** e uma **chave privada**. A chave pública é distribuída livremente para todos os correspondentes, enquanto a chave privada deve ser conhecida apenas pelo seu dono.

As mensagens criptografadas com uma das chaves só podem ser lidas com o uso da outra chave e vice-versa[44]. Ou seja, num algoritmo de criptografia assimétrica, uma mensagem cifrada com a chave pública pode somente ser decifrada pela sua chave privada correspondente. Os algoritmos de chave pública são utilizados visando a garantir a autenticidade e a confidencialidade das mensagens. Quando se trata da confidencialidade a

[41] GICO JÚNIOR , 2000a, p. 349.
[42] PINHEIRO, 2006, p.14.
[43] Idem, p. 339.
[44] Idem, p. 340.

chave pública é usada para cifrar mensagens, com isso apenas o dono da *chave privada* poderá decifrá-la. Em relação à autenticidade, a chave privada é usada para cifrar mensagens, com isso garante-se que apenas o dono da chave privada poderia ter cifrado a mensagem que foi decifrada com a "chave pública".

Sua principal vantagem é que a chave pública pode ser livremente disponibilizada como forma de garantir a autoria de determinado documento, sendo impossível que alguém falsifique a chave privada.

Os atuais programas de criptografia são capazes de cifrar um documento eletrônico e marcá-lo com uma assinatura digital de tal forma que, se houver qualquer alteração no documento, a chave pública não mais o abrirá, acusando a falsificação. As empresas responsáveis por fornecer as chaves públicas são chamadas certificadoras digitais.

Em ordenamento jurídico brasileiro, o projeto de lei 4.906/2001 já reconhece a criptografia assimétrica como instrumento de garantia de autoria e autenticidade e a define como modalidade de criptografia que utiliza um par de chaves distintas e interdependentes, denominadas chaves pública e privada, de modo que a mensagem codificada por uma das chaves só possa ser decodificada com o uso da outra chave do mesmo par.

Com a promulgação da Medida Provisória 2200-2/01, o que se percebe é que essa discussão quanto à autenticidade e integridade dos documentos digitais com assinatura digital foi superada. Essa lei, que instituiu em seu artigo primeiro[45] a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), tem como finalidade garantir a autenticidade, a integridade e a validade jurídica de documento em forma eletrônica, bem como a realização de transações eletrônicas seguras.

Quanto à presunção de veracidade dos documentos eletrônicos com o uso de processo de certificação disponibilizados pelo ICP-Brasil, dispõe o artigo 10 da referida Medida Provisória[46] que se consideram documentos públicos ou particulares, para todos os

---

45 Art. 1o Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

46 Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1o As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.

§ 2o O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

fins legais, os documentos eletrônicos de que trata esta Medida Provisória. Presumem-se, portanto, verdadeiros em relação aos signatários as declarações constantes dos documentos em forma eletrônica com a utilização de processo de certificação disponibilizado pela ICP-Brasil. Além disso, o disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Os documentos assinados dessa forma têm, portanto, valor probante *erga omnes*. Essa Medida Provisória dá uma solução jurídica para os arquivos eletrônicos com assinatura digital. Mas, o que fazer com a maioria dos arquivos, que não possuem assinatura digital? O que diz a legislação brasileira sobre esse assunto?

O artigo 371 do Código de Processo Civil dispõe que se reputa ao autor do documento particular aquele que, mandando compô-lo, não o firmou, porque conforme a experiência comum, não se costuma assinar, como livros comerciais e assentos domésticos[47]. Observe que o inciso terceiro do referido artigo presume a autoria do documento daquele que mandou produzi-lo, mesmo não tendo aposto a assinatura, desde que esteja de acordo com o senso comum.

Os arquivos eletrônicos não podem ser dissociados do meio físico em que se encontram e dependem do computador para existir. Contudo, essas características em nada diminuem a importância do documento eletrônico quando se trata de sua força probatória. Pela redação do inciso terceiro do artigo 371 do Código de Processo Civil, há presunção de veracidade dos dados ali contidos e, portanto, há validade jurídica.

Na mesma linha, o Código de Processo Civil no artigo 334 dispõe que não dependem de prova os fatos notórios; afirmados por uma parte e confessados pela parte contrária; admitidos, no processo, como incontroversos; ou, em cujo favor milita presunção legal de existência ou de veracidade[48].

---

[47] Art. 371. Reputa-se autor do documento particular:
I - aquele que o fez e o assinou;
II - aquele, por conta de quem foi feito, estando assinado;
III - aquele que, mandando compô-lo, não o firmou, porque, conforme a experiência comum, não se costuma assinar, como livros comerciais e assentos domésticos.

[48] Art. 334. Não dependem de prova os fatos:
I - notórios;
II - afirmados por uma parte e confessados pela parte contrária;
III - admitidos, no processo, como incontroversos;

O Código de Processo Penal segue no mesmo sentido, e dispõe em seu artigo 231[49] que as partes poderão apresentar documentos em qualquer fase do processo, salvo os casos expressos em lei. E no artigo 232, aduz que são documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares[50].

Quanto à convicção do juiz, o sistema probatório brasileiro baseia-se no princípio da livre apreciação das provas pelo juiz, conforme atesta o artigo 131 do Código de Processo Civil, ainda que não alegados pelas partes. Deverá, contudo, indicar, os motivos que lhe formaram o convencimento[51].

O Código de Processo Penal segue a mesma linha e dispõe em seu artigo 155, que o juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação[52].

A prova de alegação caberá a quem a fizer, sendo facultado ao juiz de ofício ordenar a produção antecipada das provas consideradas urgentes e relevantes. As provas ilícitas, bem como as derivadas das ilícitas, devem ser suprimidas do processo por serem entendidas como uma violação às normas constitucionais ou legais[53].

Assim, utilizando o princípio da livre convicção do juiz, aliado aos dispositivos apresentados, o juiz pode aplicar os referidos diplomas legais para fundamentar a utilização

---

IV - em cujo favor milita presunção legal de existência ou de veracidade.

[49] Art. 231 - Salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo.

[50] Art. 232 - Consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares.

[51] Art. 131. O juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que lhe formaram o convencimento. ,Redação dada pela Lei nº 5.925, de 1973)

[52] Art. 155. O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas

[53] Art. 156. A prova da alegação incumbirá a quem a fizer, sendo, porém, facultado ao juiz de ofício:

I – ordenar, mesmo antes de iniciada a ação penal, a produção antecipada de provas consideradas urgentes e relevantes, observando a necessidade, adequação e proporcionalidade da medida;

II – determinar, no curso da instrução, ou antes de proferir sentença, a realização de diligências para dirimir dúvida sobre ponto relevante;

Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.

§ 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.

§ 2º Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova.

dos documentos eletrônicos apresentados em sua sentença sempre que estiver convicto da autenticidade e integridade desses documentos[54].

Caso haja qualquer dúvida quanto à autenticidade, poderá ainda ser feita uma perícia técnica, da mesma forma como é feita com as representações mecânicas utilizadas como prova. O Código de Processo Civil prescreve no parágrafo único do artigo 383 que caso seja impugnada a autenticidade da reprodução mecânica, o juiz ordenará a realização de exame pericial[55].

O juiz pode proceder a uma inspeção judicial conforme prescreve o artigo 440 do CPC, e pode solicitar, se achar conveniente, a assistência de perícia nos termos do artigo 441 do CPC[56]. Segue a mesma linha o Código de Processo Penal e dispõe nos artigos 158 a 161 que quando a infração deixar vestígios será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado. Essa perícia poderá ser realizada por perito oficial e caso seja uma perícia complexa, poderá ser indicado mais de um perito oficial. Ainda, o material probatório deverá ser disponibilizado no ambiente do órgão oficial, que o manterá sempre sob sua guarda.[57]

---

§ 3º Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente.

[54] GICO JUNIOR , 2000a, p. 8.

[55] Art. 383. Qualquer reprodução mecânica, como a fotográfica, cinematográfica, fonográfica ou de outra espécie, faz prova dos fatos ou das coisas representadas, se aquele contra quem foi produzida lhe admitir a conformidade.

Parágrafo único. Impugnada a autenticidade da reprodução mecânica, o juiz ordenará a realização de exame pericial.

56 Art. 440. O juiz, de ofício ou a requerimento da parte, pode, em qualquer fase do processo, inspecionar pessoas ou coisas, a fim de se esclarecer sobre fato, que interesse à decisão da causa.

Art. 441. Ao realizar a inspeção direta, o juiz poderá ser assistido de um ou mais peritos.

[57] Art. 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.

Art. 159. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.

§ 1º Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior preferencialmente na área específica, dentre as que tiverem habilitação técnica relacionada com a natureza do exame.

§ 2º Os peritos não oficiais prestarão o compromisso de bem e fielmente desempenhar o encargo.

§ 3º Serão facultadas ao Ministério Público, ao assistente de acusação, ao ofendido, ao querelante e ao acusado a formulação de quesitos e indicação de assistente técnico.

§ 4º O assistente técnico atuará a partir de sua admissão pelo juiz e após a conclusão dos exames e elaboração do laudo pelos peritos oficiais, sendo as partes intimadas desta decisão.

§ 5º Durante o curso do processo judicial, é permitido às partes, quanto à perícia:

I – requerer a oitiva dos peritos para esclarecerem a prova ou para responderem a quesitos, desde que o mandado de intimação e os quesitos ou questões a serem esclarecidas sejam encaminhados com antecedência mínima de 10 (dez) dias, podendo apresentar as respostas em laudo complementar;

II – indicar assistentes técnicos que poderão apresentar pareceres em prazo a ser fixado pelo juiz ou ser inquiridos em audiência.

Já no âmbito do Direito Processual Penal, o artigo 235, afirma que a letra e firma dos documentos particulares serão submetidas a exame pericial, quando contestada a sua autenticidade[58]. Por sua vez, o Código de Processo Civil, no artigo 368, preceitua que se presumem verdadeiras as declarações constantes em documentos particulares em relação ao signatário[59].

É nesse contexto que a tecnologia em muito contribui para o direito à medida que fornece mecanismos para atestar identidade, autoria, integridade e acessibilidade. Caso o documento não tenha certificação digital, é possível atestar sua autenticidade e integridade por meio de perícia técnica.

Portanto, tanto os documentos eletrônicos assinados digitalmente, como aqueles que não possuem assinatura digital podem e devem ser utilizados como evidência legal, sendo que o seu grau de validade jurídica estará associado à forma como tiverem sido gerados, armazenados e preservados. Ou seja, vale reforçar que mesmo os documentos não assinados digitalmente têm valor probatório e podem ser objeto de perícia, vide os arquivos obtidos nos casos de apreensão de computadores, seja para um fim qualquer (penal, civil, tributário,...). Ainda, mesmo que as informações digitais não sejam provas em si, podem ser utilizadas ao menos como um norte para chegar a elucidação dos crimes analisados[60].

Diante da crescente expansão e disseminação dos recursos tecnológicos, torna-se imperativa, portanto, a aceitação do uso dos arquivos digitais nos processos judiciais. Assim, os arquivos digitais gerados pelos serviços de home banking, as informações comprobatórias de desvio de fluxo de caixa extraídas de computadores confiscados pelos fiscais da Receita

---

§ 6º Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes, salvo se for impossível a sua conservação.

§ 7º Tratando-se de perícia complexa que abranja mais de uma área de conhecimento especializado, poder-se-á designar a atuação de mais de um perito oficial, e a parte indicar mais de um assistente técnico.

Art. 160. Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados.

Parágrafo único. O laudo pericial será elaborado no prazo máximo de 10 dias, podendo este prazo ser prorrogado, em casos excepcionais, a requerimento dos peritos.

Art. 161. O exame de corpo de delito poderá ser feito em qualquer dia e a qualquer hora

[58] Art. 235 - A letra e firma dos documentos particulares serão submetidas a exame pericial, quando contestada a sua autenticidade.

[59] Art. 368. As declarações constantes do documento particular, escrito e assinado, ou somente assinado, presumem-se verdadeiras em relação ao signatário.

Parágrafo único. Quando, todavia, contiver declaração de ciência, relativa a determinado fato, o documento particular prova a declaração, mas não o fato declarado, competindo ao interessado em sua veracidade o ônus de provar o fato.

Federal, o material pornográfico infantil rastreado e fornecido pelos provedores de acesso são exemplos evidentes de sua força probatória e, sendo usados ou não como prova, auxiliam na formação da convicção do juiz.

Demonstrada, portanto, que a utilização dos arquivos assinados digitalmente em processo judiciais já é um tema superado, passaremos a analisar no próximo capítulo quais são os procedimentos utilizados atualmente para garantir o valor probatório dos arquivos digitais sem assinatura digital.

---

[60] PINHEIRO, 2006, p. 23.

CAPÍTULO II - VALOR PROBATÓRIO DO ARQUIVO DIGITAL

O substancial aumento de processamento dos computadores modernos, a adesão maciça dos usuários às redes mundiais e a grande expansão da comunicação sem fio em banda larga são fatores que estimulam sobremaneira a disseminação do uso da tecnologia. Além disso, o custo baixo, a facilidade de uso e a grande confiabilidade também auxiliaram a provocar uma grande revolução na sociedade em que vivemos. A criação e disseminação de máquinas de baixo custo que permitem a execução de atividades cotidianas dos desktops levaram à máxima computacional "computação em qualquer lugar e em todo lugar".

Esse grande avanço permitiu um intercâmbio de informação entre pessoas, sistemas e organizações, eliminando a grande barreira que havia para essa troca. A Internet, criada nos idos de 1960, provê uma rede global capaz de carregar qualquer tipo de informação. Em 1989, Tim Berners-Lee propôs um sistema que possibilitou a troca de informação por meio de uma interface comum conhecida como hipertexto. Essa interface permitiu a criação do que se conhece hoje como World Wide Web, sem sombra de dúvida, a inovação nos sistemas de informação mais importante do século XX.

O resultado de quarenta anos de profundas inovações é uma sociedade absolutamente dependente de tecnologia digital. Assim, tanto cidadãos de bem quanto criminosos têm igual acesso à tecnologia e dela se utilizam para realizar suas atividades. Não é de se admirar, portanto, que a utilização de computadores em práticas criminosas tenha se tornado comum. Além dos crimes tradicionais, roubo, estelionato, extorsão e tráfico de drogas, surgiu uma nova classe de crimes, os "crimes da internet", tais como a difamação e a violação de sites, o ataque a servidores, a disseminação de falsos e-mails, o roubo de dados ("phishing scan"), a disseminação de vírus de computador, as retiradas e transferências de contas bancárias, dentre outros.

Essa realidade demanda um conhecimento técnico cada vez maior na identificação de vestígios e aumenta o grau de importância da Informática na comprovação de seu valor probatório na Justiça. Tornou-se comum, portanto, considerar se há algum dispositivo digital que contenha informações relacionadas aos crimes cometidos. Ainda que não tenha havido uma participação direta na cena do crime, seu uso por um dos envolvidos pode agregar

importantes informações para sua elucidação. Por exemplo, a utilização de celulares ou o envio e recebimento de mensagens de e-mails são fontes de informação que podem levar à resolução de alguns crimes.

No caso de um computador estar sob suspeita, os vestígios encontrados atestam de forma direta a realização do crime, sejam eles programas ou arquivos, ao contrário de crimes fora do ambiente computacional, que apenas levam a interpretações quanto aos fatos que podem ter ocorrido antes de sua consumação[61].

Diante do exposto, tornou-se possível utilizar softwares e computadores potentes na identificação de criminosos, rastrear evidências em ligações telefônicas, aprimorar ou ampliar imagens de cenas de um crime, dentre outras inúmeras possibilidades que podem facilitar a elucidação de um crime[62].

Como já exposto no capítulo anterior, arquivos eletrônicos podem ser certificados ou não. Quando certificados, não há questionamento quanto à autenticidade e à integridade, tendo essa questão sido superada com a promulgação da Medida Provisória 2200-2/01 que instituiu a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil). Contudo, mais de noventa por cento dos arquivos que trafegam digitalmente não possuem certificação digital. Paira então a pergunta sobre o que fazer com esses arquivos? Como garantir a sua utilização em processos judiciais sem comprometer o devido processo legal? A Forense Digital, subárea da Ciência Forense, nos traz a resposta para essas inquietudes.

1) Ciência Forense

Como ciência auxiliar do Direito Penal, o papel fundamental da Ciência Forense é identificar os vestígios caracterizadores do delito, estudá-los e interpretá-los de forma a viabilizar a ação da Justiça. Nesse sentido, torna-se importante obter o valor probatório, coerente com as regras e leis admissíveis em uma corte de Justiça criminal.

Tida como ciência multidisciplinar, se vale do conhecimento de diversas outras áreas para viabilizar a análise de um dado vestígio. A Papiloscopia, a Medicina Legal, a Patologia Forense, a Antropologia, a Psiquiatria Forense, a Odontologia Forense, a Engenharia, a Balística, dentre outros, são exemplos de áreas que auxiliam a Ciência Forense

[61] CALAZANS & CALAZANS , 2005, p.11.
[62] Idem , p.10.

na elucidação de crimes. Assim, em cada perícia a ser realizada, a que considerar os conhecimentos e técnicas necessários para analisar as evidências detectadas.

Disciplina da Ciência Forense, a Forense Digital é definida como uma área de conhecimento que se utiliza de métodos elaborados e comprovados cientificamente, visando a preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais, e surge com o propósito de facilitar ou permitir a reconstituição de procedimentos de natureza criminosa que ocorram em equipamentos digitais. Trabalha com informações armazenadas ou transmitidas por equipamentos digitais como telefones celulares, máquinas de FAX, centrais telefônicas digitais, computadores, dentre outros.[63]

A Forense Computacional é definida por Pires como:

> *"A Ciência Forense Computacional é um conjunto de técnicas, cientificamente comprovadas, utilizadas para coletar, reunir, identificar, examinar, correlacionar, analisar e documentar evidências digitais processadas, armazenadas ou transmitidas por computadores."* [64]

Nas palavras de Martinez, proporciona:

> *"Os princípios e técnicas que facilitam a investigação do delito; em outras palavras, qualquer princípio ou técnica que pode ser aplicada para identificar, recuperar, reconstruir ou analisar a evidência durante uma investigação criminal, é parte da Ciência Forense"* [65].

É amplamente utilizada no Direito Penal, como instrumento para agregar valor probatório às evidências detectadas, bem como instrumento de resposta a incidentes, visando resguardar a segurança e a confiabilidade dos sistemas em execução em grandes corporações.

Quando se trata de resposta a incidentes, refere-se ao exame realizado em uma corporação com o objetivo de determinar a causa do incidente, buscando evitar sua reincidência. Nesse caso, não há a preocupação com as formalidades legais. Essa segunda linha não faz parte do escopo do presente trabalho.

Face ao grau de complexidade dos sistemas e softwares a serem analisados, torna-se necessário que os profissionais da área, ou seja, os analistas de sistemas sejam os

[63] CALAZANS & CALAZANS , 2005, p. 10.
[64] PIRES , 2003, p. 55.

responsáveis pelas investigações forenses nesse campo. Além disso, há que utilizar as ferramentas adequadas, evitando assim que qualquer procedimento comprometa as evidências a serem examinadas. Na análise de uma máquina, são utilizadas ferramentas específicas com o objetivo de não modificar o sistema em investigação.

2) Breve histórico

A maior parte dos métodos e dos instrumentos forenses surgiu no período compreendido entre os séculos XVI e XVIII. As armas de fogo começaram a ser produzidas com almas raiadas[66] no final do século XVIII, o que permitiu que Henry Godard pudesse relacionar uma bala à arma utilizada no século posterior[67]. Criada em 1826, a fotografia tornou possível o registro dos fatos ocorridos no local do crime, bem como o reconhecimento de suspeitos.

Ainda que muitos dos recursos criados nessa época tenham se tornado obsoletos, muitos dos conceitos se tornaram basilares para diversas áreas da Ciência Forense, dentre elas a Balística e a Toxicologia.

Diversos estudiosos muito contribuíram para a construção dessa ciência, mas foi Edmond Locard, um médico francês, que provocou uma verdadeira revolução na metodologia de investigação criminal. Ele definiu o princípio fundamental da Ciência Forense conhecido como ***Princípio de Intercâmbio*** ou ***Princípio de Locard*** que estabelece "que quando um indivíduo entra em contato com um objeto ou outro indivíduo, sempre deixa vestígio desse contato" [68]. Criador da conhecida Poroscopia (Estudo dos poros), Edmond Locard sistematizou a investigação criminal, ao definir métodos para recolhimento e análise de vestígios.

---

[65] MARTINEZ , 2005, p. 99.
[66] A alma é raiada quando o interior do cano tem sulcos helicoidais dispostos no eixo longitudinal, destinados a forçar o projétil a um movimento de rotação.
[67] CALAZANS & CALAZANS, 2005.
[68] Idem, p. 5.

3) Amparo da legislação brasileira

O sistema probatório brasileiro baseia-se no princípio da livre apreciação das provas pelo juiz, conforme atesta o artigo 131 do Código de Processo Civil. Deverá, contudo, indicar, os motivos que lhe formaram o convencimento[69]. O Código de Processo Penal segue a mesma linha e dispõe em seu artigo 155, que o juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação[70].

Diante da ausência de normas específicas na legislação brasileira para a investigação em âmbito computacional, as normas gerais para todo tipo de perícia criminal definidas no Código de Processo Penal dos artigos 158 a 184 devem ser adotadas[71], com o fito de garantir que os vestígios encontrados possam ter algum valor probatório.

---

[69] Art. 131. O juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que Ihe formaram o convencimento.

[70] Art. 155. O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas

[71] Art. 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.

Art. 159. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.

§ 1º Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior preferencialmente na área específica, dentre as que tiverem habilitação técnica relacionada com a natureza do exame.

§ 2º Os peritos não oficiais prestarão o compromisso de bem e fielmente desempenhar o encargo. § 3º Serão facultadas ao Ministério Público, ao assistente de acusação, ao ofendido, ao querelante e ao acusado a formulação de quesitos e indicação de assistente técnico.

§ 4º O assistente técnico atuará a partir de sua admissão pelo juiz e após a conclusão dos exames e elaboração do laudo pelos peritos oficiais, sendo as partes intimadas desta decisão.

§ 5º Durante o curso do processo judicial, é permitido às partes, quanto à perícia:

I – requerer a oitiva dos peritos para esclarecerem a prova ou para responderem a quesitos, desde que o mandado de intimação e os quesitos ou questões a serem esclarecidas sejam encaminhados com antecedência mínima de 10 (dez) dias, podendo apresentar as respostas em laudo complementar;

II – indicar assistentes técnicos que poderão apresentar pareceres em prazo a ser fixado pelo juiz ou ser inquiridos em audiência.

§ 6º Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes, salvo se for impossível a sua conservação.

§ 7º Tratando-se de perícia complexa que abranja mais de uma área de conhecimento especializado, poder-se-á designar a atuação de mais de um perito oficial, e a parte indicar mais de um assistente técnico.

Art. 160. Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados.

Parágrafo único. O laudo pericial será elaborado no prazo máximo de 10 dias, podendo este prazo ser prorrogado, em casos excepcionais, a requerimento dos peritos.

Art. 161. O exame de corpo de delito poderá ser feito em qualquer dia e a qualquer hora.

Assim, utilizando o princípio da livre convicção do juiz, o juiz pode aplicar os referidos diplomas legais para fundamentar a utilização dos arquivos digitais apresentados[72]. Caso haja qualquer dúvida quanto à autenticidade, poderá ainda ser feita uma perícia técnica, da mesma forma como é feita com as representações mecânicas utilizadas como prova.

O artigo 158 estabelece que, quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior. Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior preferencialmente na área específica. É permitido no curso do processo, requerer a oitiva da perícia com o fito de

---

Art. 167. Não sendo possível o exame de corpo de delito, por haverem desaparecido os vestígios, a prova testemunhal poderá suprir-lhe a falta.

Art. 169. Para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos.

Parágrafo único. Os peritos registrarão, no laudo, as alterações do estado das coisas e discutirão, no relatório, as conseqüências dessas alterações na dinâmica dos fatos.

Art. 170. Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.

Art. 171. Nos crimes cometidos com destruição ou rompimento de obstáculo a subtração da coisa, ou por meio de escalada, os peritos, além de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado.

Art. 172. Proceder-se-á, quando necessário, à avaliação de coisas destruídas, deterioradas ou que constituam produto do crime.

Parágrafo único. Se impossível a avaliação direta, os peritos procederão à avaliação por meio dos elementos existentes nos autos e dos que resultarem de diligências.

Art. 175. Serão sujeitos a exame os instrumentos empregados para a prática da infração, a fim de se Ihes verificar a natureza e a eficiência.

Art. 176. A autoridade e as partes poderão formular quesitos até o ato da diligência.

Art. 178. No caso do art. 159, o exame será requisitado pela autoridade ao diretor da repartição, juntando-se ao processo o laudo assinado pelos peritos.

Art. 179. No caso do § 1º do art. 159, o escrivão lavrará o auto respectivo, que será assinado pelos peritos e, se presente ao exame, também pela autoridade.

Parágrafo único. No caso do art. 160, parágrafo único, o laudo, que poderá ser datilografado, será subscrito e rubricado em suas folhas por todos os peritos.

Art. 180. Se houver divergência entre os peritos, serão consignadas no auto do exame as declarações e respostas de um e de outro, ou cada um redigirá separadamente o seu laudo, e a autoridade nomeará um terceiro; se este divergir de ambos, a autoridade poderá mandar proceder a novo exame por outros peritos.

Art. 181. No caso de inobservância de formalidades, ou no caso de omissões, obscuridades ou contradições, a autoridade judiciária mandará suprir a formalidade, complementar ou esclarecer o laudo.

Parágrafo único. A autoridade poderá também ordenar que se proceda a novo exame, por outros peritos, se julgar conveniente.

Art. 182. O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte.

Art. 183. Nos crimes em que não couber ação pública, observar-se-á o disposto no art. 19.

Art. 184. Salvo o caso de exame de corpo de delito, o juiz ou a autoridade policial negará a perícia requerida pelas partes, quando não for necessária ao esclarecimento da verdade.

[72] GICO JUNIOR , 2000a, p. 8.

esclarecer questões obscuras. O material probatório será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda.Tratando-se de perícia complexa que abranja mais de uma área de conhecimento especializado, poder-se-á designar a atuação de mais de um perito oficial, e a parte indicar mais de um assistente técnico.

O artigo 169 dispõe que para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos. No parágrafo único, os peritos registrarão, no laudo, as alterações do estado das coisas e discutirão, no relatório, as conseqüências dessas alterações na dinâmica dos fatos.

Quanto às perícias de laboratório, o artigo 170 dispõe que os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquema. Caso haja divergência entre os peritos, serão consignadas no auto do exame as declarações e respostas de um e de outro, ou cada um redigirá separadamente o seu laudo, e a autoridade nomeará um terceiro; se este divergir de ambos, a autoridade poderá mandar proceder a novo exame por outros peritos.

Estabelece ainda em seu artigo 332 que são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa, todos os meios legais, bem como os moralmente legítimos, ainda que não especificados pelo código. Dispõe o artigo 335 que o juiz aplicará as regras de experiência comum subministradas pela observação do que ordinariamente acontece e ainda as regras da experiência técnica, ressalvado, quanto a esta, o exame pericial. O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte.

O Código de Processo Civil segue na mesma linha e estabelece nos artigos 145 e 421 do Código de Processo Civil que quando a prova do fato depender de conhecimento técnico ou científico, o juiz será assistido por perito, que deverá entregar o laudo no prazo fixado pelo juiz, podendo ser responsabilizado por quaisquer informações inverídicas que prestar[73].

---

[73] Seção II - Do Perito

Art. 145. Quando a prova do fato depender de conhecimento técnico ou científico, o juiz será assistido por perito, segundo o disposto no art. 421.

§ 1o Os peritos serão escolhidos entre profissionais de nível universitário, devidamente inscritos no órgão de classe competente, respeitado o disposto no Capítulo Vl, seção Vll, deste Código.

Para o bom desempenho da função, poderão o perito e os assistentes técnicos utilizar todos os meios necessários, ouvindo testemunhas, obtendo informações, solicitando documentos que estejam em poder de parte ou em repartições públicas, bem como instruir o laudo com plantas, desenhos, fotografias e outras quaisquer peças, segundo rege o artigo 429 do CPC[74].

---

§ 2o Os peritos comprovarão sua especialidade na matéria sobre que deverão opinar, mediante certidão do órgão profissional em que estiverem inscritos.

§ 3o Nas localidades onde não houver profissionais qualificados que preencham os requisitos dos parágrafos anteriores, a indicação dos peritos será de livre escolha do juiz.

Art. 146. O perito tem o dever de cumprir o ofício, no prazo que Ihe assina a lei, empregando toda a sua diligência; pode, todavia, escusar-se do encargo alegando motivo legítimo.

Parágrafo único. A escusa será apresentada dentro de 5 (cinco) dias, contados da intimação ou do impedimento superveniente, sob pena de se reputar renunciado o direito a alegá-la (art. 423).

Art. 147. O perito que, por dolo ou culpa, prestar informações inverídicas, responderá pelos prejuízos que causar à parte, ficará inabilitado, por 2 (dois) anos, a funcionar em outras perícias e incorrerá na sanção que a lei penal estabelecer.

74 Seção VII - Da Prova Pericial

Art. 420. A prova pericial consiste em exame, vistoria ou avaliação.

Parágrafo único. O juiz indeferirá a perícia quando:

I - a prova do fato não depender do conhecimento especial de técnico;

II - for desnecessária em vista de outras provas produzidas;

III - a verificação for impraticável.

Art. 421. O juiz nomeará o perito, fixando de imediato o prazo para a entrega do laudo.

§ 1o Incumbe às partes, dentro em 5 (cinco) dias, contados da intimação do despacho de nomeação do perito:

I - indicar o assistente técnico;

II - apresentar quesitos.

§ 2o Quando a natureza do fato o permitir, a perícia poderá consistir apenas na inquirição pelo juiz do perito e dos assistentes, por ocasião da audiência de instrução e julgamento a respeito das coisas que houverem informalmente examinado ou avaliado.

Art. 422. O perito cumprirá escrupulosamente o encargo que Ihe foi cometido, independentemente de termo de compromisso. Os assistentes técnicos são de confiança da parte, não sujeitos a impedimento ou suspeição.

Art. 423. O perito pode escusar-se (art. 146), ou ser recusado por impedimento ou suspeição (art. 138, III); ao aceitar a escusa ou julgar procedente a impugnação, o juiz nomeará novo perito.

Art. 426. Compete ao juiz:

I - indeferir quesitos impertinentes;

II - formular os que entender necessários ao esclarecimento da causa.

Art. 427. O juiz poderá dispensar prova pericial quando as partes, na inicial e na contestação, apresentarem sobre as questões de fato pareceres técnicos ou documentos elucidativos que considerar suficientes.

Art. 429. Para o desempenho de sua função, podem o perito e os assistentes técnicos utilizar-se de todos os meios necessários, ouvindo testemunhas, obtendo informações, solicitando documentos que estejam em poder de parte ou em repartições públicas, bem como instruir o laudo com plantas, desenhos, fotografias e outras quaisquer peças.

Art. 431-A. As partes terão ciência da data e local designados pelo juiz ou indicados pelo perito para ter início a produção da prova.

Art. 431-B. Tratando-se de perícia complexa, que abranja mais de uma área de conhecimento especializado, o juiz poderá nomear mais de um perito e a parte indicar mais de um assistente técnico.

Quanto ao exame pericial, a perícia em informática é responsável, portanto, por produzir laudos periciais com o objetivo de determinar a dinâmica, a materialidade e a autoria dos atos ilícitos. Assim, tem como principal finalidade identificar, processar e transformar evidências digitais em provas materiais de crimes utilizando métodos técnico-científicos, com o objetivo precípuo de conferir-lhes validade probatória em juízo.

4) Perícia em Informática

Tanto o Código de Processo Civil como o Código de Processo Penal estabelecem que quando a prova do fato depender de conhecimento técnico ou científico, o juiz será assistido por perito, que deverá entregar o laudo no prazo fixado pelo juiz.

Essa prova pericial consiste em exame, vistoria ou avaliação. A critério do juiz, a perícia poderá ser indeferida quando a prova do fato não depender do conhecimento especial de técnico; for desnecessária em vista de outras provas produzidas; ou, a verificação se mostrar impraticável.

Art. 432. Se o perito, por motivo justificado, não puder apresentar o laudo dentro do prazo, o juiz conceder-lhe-á, por uma vez, prorrogação, segundo o seu prudente arbítrio.

Art. 433. O perito apresentará o laudo em cartório, no prazo fixado pelo juiz, pelo menos 20 (vinte) dias antes da audiência de instrução e julgamento.

Parágrafo único. Os assistentes técnicos oferecerão seus pareceres no prazo comum de 10 (dez) dias, após intimadas as partes da apresentação do laudo.

Art. 434. Quando o exame tiver por objeto a autenticidade ou a falsidade de documento, ou for de natureza médico-legal, o perito será escolhido, de preferência, entre os técnicos dos estabelecimentos oficiais especializados. O juiz autorizará a remessa dos autos, bem como do material sujeito a exame, ao diretor do estabelecimento.

Parágrafo único. Quando o exame tiver por objeto a autenticidade da letra e firma, o perito poderá requisitar, para efeito de comparação, documentos existentes em repartições públicas; na falta destes, poderá requerer ao juiz que a pessoa, a quem se atribuir a autoria do documento, lance em folha de papel, por cópia, ou sob ditado, dizeres diferentes, para fins de comparação.

Art. 435. A parte, que desejar esclarecimento do perito e do assistente técnico, requererá ao juiz que mande intimá-lo a comparecer à audiência, formulando desde logo as perguntas, sob forma de quesitos.

Parágrafo único. O perito e o assistente técnico só estarão obrigados a prestar os esclarecimentos a que se refere este artigo, quando intimados 5 (cinco) dias antes da audiência.

Art. 436. O juiz não está adstrito ao laudo pericial, podendo formar a sua convicção com outros elementos ou fatos provados nos autos.

Art. 437. O juiz poderá determinar, de ofício ou a requerimento da parte, a realização de nova perícia, quando a matéria não Ihe parecer suficientemente esclarecida.

Art. 438. A segunda perícia tem por objeto os mesmos fatos sobre que recaiu a primeira e destina-se a corrigir eventual omissão ou inexatidão dos resultados a que esta conduziu.

Art. 439. A segunda perícia rege-se pelas disposições estabelecidas para a primeira.

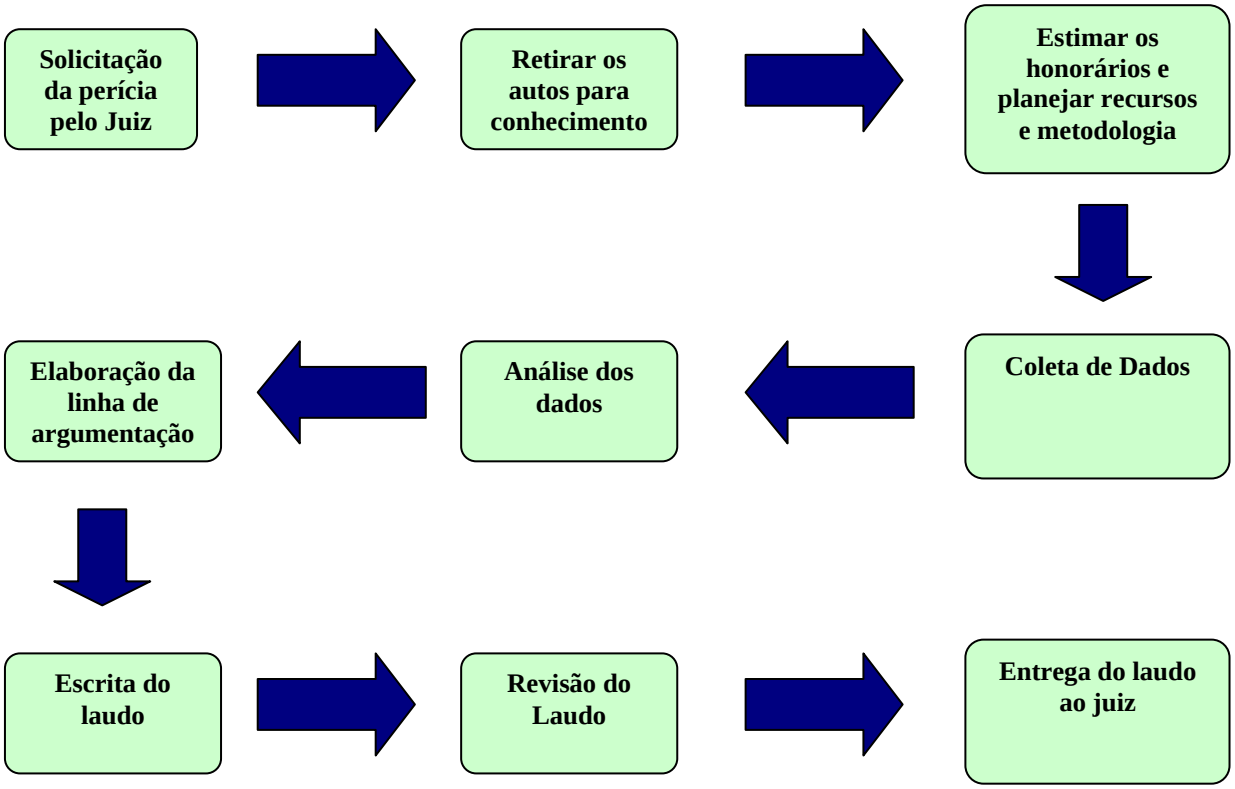
Parágrafo único. A segunda perícia não substitui a primeira, cabendo ao juiz apreciar livremente o valor de uma e outra.

Para o bom desempenho da função, poderão o perito e os assistentes técnicos utilizar todos os meios necessários, ouvindo testemunhas, obtendo informações, solicitando documentos que estejam em poder de parte ou em repartições públicas, bem como instruir o laudo com plantas, desenhos, fotografias e outras quaisquer peças.

A reconstrução dos eventos e elaboração de conclusões acerca dos atos ilícitos requer muito mais do que a simples identificação de evidências isoladas nas diversas fontes de informação. É necessário correlacionar as informações extraídas, seja para corroborar uma suspeita ou para identificar novas pistas.

Nesse sentido, torna-se importante detalhar minuciosamente as informações detectadas com o objetivo de permitir inter-relacionar as evidências encontradas no sistema em análise. Assim, a construção de uma linha do tempo e de gráficos relacionais podem ajudar o investigador a identificar com maior clareza a ordem dos eventos, bem como, descobrir novas evidências.

Zochio, baseando-se em SANTOS e MELO (2004), apresenta o seguinte ciclo de elaboração do laudo pericial:



Ciclo de Elaboração de Laudo Pericial - Zochio (2010:28)

O processo de perícia em informática começa, por conseguinte, a partir de um mandado judicial. Daí é feita a coleta no local do crime, a apreensão, a preservação do material coletado, a duplicação do material coletado, a análise que é feita nas cópias e, por fim, a documentação da análise que é colocada em um Laudo Pericial.

Para tanto, torna-se premente que a perícia seja feita de forma planejada considerando os seguintes fatores relevantes na execução dos trabalhos periciais:

a) "conhecimento detalhado dos fatos concernentes à lide;
b) as diligências a serem realizadas;
c) os locais, equipamentos, documentos e vestígios a serem examinados e coletados;
d) a natureza, a oportunidade e a extensão dos procedimentos de perícia a serem aplicados;
e) a equipe técnica necessária à execução do trabalho;
f) os serviços especializados, necessários à execução do trabalho;
g) os quesitos, quando formulados;
h) o tempo necessário para elaboração do trabalho" [75].

5) Evidência Digital

No caso de crimes cibernéticos, as evidências podem estar presentes em mensagens de correio eletrônico e bate-papo, imagens de pornografia infantil, dados cifrados, registros de impressão, engenharia reversa de programas, conversão de banco de dados, registros de conexão à Internet e fragmentos de arquivos. A perícia pode ser realizada em mídias digitais, máquinas caça-níqueis, aparelhos celulares, ou mesmo na Internet.

Qualquer pedaço de dado ou software em um sistema digital pode ser uma evidência, se ele tem algum significado relevante para a investigação. Deve-se lembrar que informações existem porque foram úteis a alguma atividade humana.

Entende-se por evidência digital qualquer informação armazenada ou transmitida no formato digital, composta de campos magnéticos e pulsos eletrônicos que podem ser coletados e analisados por meio de ferramentas adequadas. Essas evidências podem ser duplicadas, o que permite a preservação da evidência original. Além disso, com os métodos

[75] ZOCHIO, 2010, p. 30.

existentes, é muito fácil identificar se foi modificada ou não. Por outro lado, é altamente volátil, podendo ser modificada facilmente durante sua análise[76].

Marshall[77] defende que as evidências digitais podem ser encontradas em dispositivos digitais em ***Sistemas Abertos*** ou em ***Sistemas Fechados***. Qualquer sistema que nunca tenha sido conectado à Internet, subsistente em um ambiente totalmente controlado e conhecido, é definido como ***Sistema Fechado***. O ***Sistema Aberto***, por sua vez, independe do tamanho e requer que tenha sido feita conexão com a Internet, o que pode ter sido de forma direta (p.e., rede sem fio pública) ou indireta (p.e., dispositivo de memória auxiliar USB). São fontes muito mais ricas de informação quanto a pessoas, atividades, hábitos e interesses. Um complicador para esses sistemas refere-se à determinação do local de ocorrência do crime. Uma vez que a rede é internacional, sua ocorrência pode se dar em qualquer lugar do planeta. Ocorre que as legislações não são uniformizadas e a categorização como crime vai depender da localidade em análise.

A importância dessa distinção reside no fato de que sistemas abertos estão sujeitos a intervenções externas e, por conseqüência, apresentam um grau maior de incerteza quanto à compreensão do problema apresentado.

Com o fito de analisar os dispositivos digitais existentes e identificar as evidências, o autor propõe um esquema de análise desses dispositivos. A princípio, deve-se identificar quem assume os seguintes papéis: testemunha, ferramenta, cúmplice, guardião e vítima.

A ***testemunha*** é um observador passivo da atividade. Não tem contato com os participantes, mas pode descrever o fato com determinado grau de detalhes. Um Circuito fechado de televisão é um exemplo dessa categoria. A ***ferramenta*** representa alguma coisa não essencial, que torna a atividade mais fácil. Pode ser um programa, um dispositivo individual ou uma rede de computadores, por exemplo. Os ***cúmplices*** são participantes essenciais ao sucesso das atividades, sejam coagidos ou não. A ***vítima*** é o alvo do ataque, em geral são pessoas ou corporações. E, por fim, o ***guardião*** que pode executar algumas das funções de um tutor.

Qualquer dispositivo digital pode assumir vários papéis dentro de uma atividade. As categorias supracitadas são importantes para avaliar seu potencial como prova em uma

[76] REIS & GEUS, 2001, p. 6.
[77] MARSHALL, 2008, p.52.

determinada situação. O autor sugere que seja feita uma tabela como esta para cada ocorrência criminosa, buscando se concentrar naqueles dispositivos que tenham mais dados relevantes. Não há como fazer essa definição antes de avaliar os dispositivos. Logo, como regra básica e número um, torna-se obrigatório criar uma imagem de todos os dispositivos digitais envolvidos para que possam ser avaliados em momento posterior e para garantir que os dados originais não sejam alterados.

Tabela I – Papéis desempenhados por um dispositivo digital[78]

	Testemunha	***Ferramenta***	***Cúmplice***	***Guardião***	***Vítima***
Sistema Fechado	Testemunha em sistema Fechado (TF)	Ferramenta em sistema Fechado (FF)	Cúmplice em sistema Fechado (CF)	Guardião em sistema Fechado (GF)	Vítima em sistema Fechado (VF)
Sistema Aberto	Testemunha em sistema Aberto (TA)	Ferramenta em sistema Aberto (TA)	Cúmplice em sistema Aberto (CA)	Guardião em sistema Aberto (GA)	Vítima em sistema Aberto (VA)

Com o objetivo de auxiliar a identificar as evidências nos dispositivos digitais, Marshall ainda propõe dois outros modelos. O primeiro modelo, baseado em segurança, possui sete elementos:

a) ***Entidades***: São objetos que podem manipular ou ser manipulados pelo sistema e podem ser passivos ou ativos. Podem ser pessoas, organizações ou outros tipos de objetos. Do ponto de vista investigativo, ou são os usuários do sistema ou os potenciais alvos dos criminosos.

b) ***Ambiente***: Representa o conjunto de regras ou restrições impostas às entidades com o objetivo de fazê-las agir corretamente. Pode ser definido em termos de legislação, regras, capacidade técnica, limitações de recursos, limitações físicas, dentre outros.

c) ***Organização***: Contém o framework que permite que as regras e controles sejam criados permitindo, assim, que as entidades cooperem e colaborem tanto quanto possível.

d) ***Infra-instrutora***: Mecanismo de suporte necessário para permitir que as atividades ocorram dentro da organização. Do ponto de vista investigativo, representa a "cena do crime"

[78] MARSHALL, 2008, p. 13.

a onde as informações serão procuradas. Torna-se, portanto, importante saber como está estruturada, para identificar os limites dos componentes críticos.

e) ***Atividades***: São as tarefas executadas.

f) ***Procedimentos***: São tarefas simples que representam processos atômicos e indivisíveis em um contexto de uma atividade.

g) ***Dados***: A representação das entidades que o sistema está preocupado em manipular. Qualquer falha na segurança dos dados torna o sistema vulnerável.

Por meio de um sistema que utilize esse modelo de sete elementos, torna-se possível identificar a onde residem as fragilidades do sistema, o que facilita levantar quais partes permitem a ocorrências de atividades não desejadas.

Outro modelo, contudo, permitirá entender como essa atividade ocorreu e definir o grau de responsabilidade do usuário envolvido.

Tabela II - Grau de responsabilidade do usuário envolvido

	Ato conhecido	***Ato não conhecido***
Usuário autorizado	Usuário autorizado executa ato conhecido (AK)	Usuário autorizado executa ato acidentalmente (AU)
Usuário não autorizado	Usuário não autorizado executa ato conhecido (UK)	Usuário não autorizado executa ato acidentalmente (UU)

O vetor ***Ato conhecido*** refere-se a atividades sob as quais o usuário está consciente quanto às conseqüências de suas ações. Por exemplo, atos onde o usuário deliberadamente implantou um software ilícito no sistema. No caso de consumo de material ilegal, determinar se o usuário conhecia o ato que estava executando é essencial para a acusação em um processo judicial.

O vetor **Ato não conhecido** refere-se a atividades sob as quais o usuário não está consciente quanto às conseqüências de suas ações. No caso de processos envolvendo crianças abusadas, uma questão substancial é saber se a imagem em questão foi ou não implantada por

um vírus ou um pop-up de uma página da web. Isso implica dizer se o ato era conhecido ou não conhecido.

Há diversas formas de um ato não conhecido ser executado em um computador de um usuário autorizado: (1) efeito de web-site; (2) download de arquivos compactados; (3) compartilhamento de arquivos; (4) Softwares com comportamentos indesejados, por exemplo, vírus, cavalos de tróia, dentre outros.

Os modelos apresentados são exemplos de como o perito pode estudar e buscar as evidências no material coletado para análise, bem como direcionar o trabalho de análise. O modelo que relaciona papéis desempenhados por um determinado dispositivo digital é importante para avaliar o potencial de cada dispositivo como prova em uma determinada situação. O autor sugere que seja feita uma tabela como esta para cada ocorrência criminosa, buscando se concentrar naqueles dispositivos que tenham mais dados relevantes. O modelo dos sete elementos permite identificar as fragilidades do sistema e suas vulnerabilidades. Por fim, o terceiro modelo apresentado permite detectar o grau de responsabilidade de cada usuário na atividade realizada. Esses modelos são usados na fase de análise das evidências digitais.

6) Ordem de volatilidade das evidências digitais

A ordem de volatilidade, conceito definido por Dan Farmer e Wietse Venema, determina que o tempo de vida de uma evidência digital varia de acordo com o local onde está armazenada. Na ordem descendente de volatilidade, as principais fontes de informação são apresentadas como segue:

a) dispositivos de armazenagem da CPU;
b) memória de periféricos;
c) memória principal do sistema;
d) tráfego de rede;
e) estado do sistema operacional;
f) dispositivos de armazenagem secundária.

Quanto maior a volatilidade de uma determinada informação, mais difícil se torna sua extração e menos tempo há para capturá-la. Informações voláteis tais como o conteúdo da

memória principal e dos dispositivos de armazenagem secundária, bem como, o estado do sistema operacional podem conter informações valiosas a respeito dos atos ilícitos cometidos e podem determinar seus responsáveis.

As informações contidas nos ***dispositivos de armazenagem da CPU***, cuja captura é praticamente impossível, são de mínima utilidade. Os *caches* contêm informações ainda não gravadas na memória principal, mas é impossível obter essas informações face ao seu alto grau de volatilidade[79].

As ***memórias periféricas,*** relativas a modems, pagers, aparelhos de fax e impressoras, dentre outras, contêm informações que não residem no sistema analisado, mas que podem ser acessadas e salvas, tais como documentos e mensagens de texto ou número de fax e telefones[80].

A captura do ***tráfego em rede*** pode ser comparada à gravação em vídeo de um crime. Nesse caso, são capturados datagramas que permitem a reconstrução da comunicação entre os alvos analisados. Os programas responsáveis por gerar esses **datagramas** são conhecidos por *sniffers*[81].

Os sniffers são capazes de capturar os datagramas que trafegam na rede, podem decodificá-los e exibi-los em formato mais legível, ou ainda recuperar arquivos transferidos pela rede. O exemplo mais comum dessa ferramenta é o *TCPDUMP*[82]. A prática mais recomendada para a coleta de informações é a captura dos datagramas em seu estado original no formato binário. Isso evita a perda de informações. Contudo, isso nem sempre é possível, em especial, quando há necessidade de analisar o tráfego de rede em tempo real.

A análise dos datagramas capturados pode ser feita com o auxílio de ferramentas que reconstroem as informações em um formato mais legível, tais como a ethereal[83] e o review. O volume de tráfego de rede pode ser muito grande, logo a análise pode centrar-se nos tipos mais comuns utilizados pelos criminosos: HTTP, IRQ, SMTP, RPC, por exemplo.

Informações do ***estado do sistema operacional*** representam uma imagem do sistema operacional em um dado instante e geralmente são perdidas quando o sistema é desligado. Geralmente, apresentam informações preciosas quanto a ocorrência de atos ilícitos.

---

[79] REIS & GEUS, 2001, p. 58.
[80] Idem, p. 59.
[81] Idem, p. 59.
[82] Para obter mais informações, acesse o site HTTP://www.tcpdump.org .
[83] Para obter mais informações, acesse o site HTTP://www.ethereal.com .

Podem indicar, portanto, existência de processos com nomes suspeitos ou acesso a arquivos suspeitos, por exemplo.

Os ***dispositivos de armazenagem secundária*** representam a maior fonte de informação para a análise forense. Além de ser uma memória não volátil, sua capacidade de armazenamento é enorme. Cada porção de memória do dispositivo de armazenagem representa uma fonte de informação em potencial. Podem-se dividir essas informações em áreas acessíveis pelo sistema de arquivos e áreas não acessíveis pelo sistema.

As ***áreas não acessíveis pelo sistema de arquivos*** podem conter tanto informações deliberadamente escondidas, quanto informações deletadas. Quando um arquivo é deletado, sua referência é removida da estrutura do sistema de arquivos, mas os dados contidos não são apagados do disco. Esses dados permanecem lá até serem sobrescritos por outros arquivos. Assim, arquivos completos ou partes podem ser recuperados mesmo após terem sido deletados.

O ***sistema de arquivos*** é a fonte de informação básica para a análise forense. Como banco de dados, é a parte do sistema operacional responsável por organizar as informações do disco na forma de arquivos. Cada sistema operacional possui a sua forma de organizar os arquivos. A quantidade e a qualidade das pistas deixadas nas estruturas de dados do sistema de arquivos irá determinar o número de informações que podem ser recuperados sobre um arquivo deletado.

Para se ter acesso aos arquivos e diretórios do ***sistema de arquivos*** analisado é preciso antes montá-lo no sistema de análise. Uma vez preparado e montado, é possível buscar as evidências dos atos ilícitos. As principais fontes de informação contidas em um sistema de arquivos são arquivos e diretórios de configuração; informações sobre processos em execução e atividades incompletas; arquivos de cache que podem conter, por exemplo, histórico de sites Web acessados; arquivos de swap[84]; diretórios temporários; arquivos e diretórios não usuais ou escondidos; executáveis e bibliotecas; arquivos de log que permitem a reconstituição de fatos que ocorreram no sistema; e, por fim, arquivos e diretórios dos usuários[85].

---

[84] "Quando a demanda do sistema excede a capacidade de memória, algumas informações são retiradas da memória e armazenadas temporariamente nos arquivos de swap. Tais arquivos podem conter fragmentos de dados ou até mesmo um arquivo completo que nunca foi salvo antes." (REIS & GEUS, 2001, p. 37)

[85] REIS & GEUS, 2001, ps. 37 e 38.

7) Princípios e Boas Práticas na Investigação Forense

Em um julgamento, garantir a continuidade das evidências é essencial para a formação da convicção do juiz ou do júri. Qualquer dúvida quanto a essa continuidade, pode levar à invalidade da prova.

Assim, para garantir que os resultados da investigação forense tenham valor probatório, torna-se essencial seguir determinados protocolos que assegurem que as evidências sejam coletadas, preservadas e analisadas de forma minuciosa e livre de contaminações. Esses procedimentos, definidos pelo termo Standard Operation Procedures[86] (SOP), são um guia prático e documentado, que imprimem um controle de qualidade nas análises realizadas, que devem ser detalhadas, documentadas, revisadas e aceitas por comunidade científica relevante.

Com o objetivo de garantir a autenticidade e a integridade das evidências digitais analisadas, os procedimentos adotados no processo de investigação forense devem atender aos princípios e boas práticas dos profissionais da área. Nesse sentido, dois grupos são de fundamental importância para o direcionamento dos trabalhos da área: a Associação de Oficiais Chefes de Polícia do Reino Unido (ACPO) [87] e o Grupo de Trabalho Científico em Evidências Digitais (SWGDE) [88].

A associação dos Oficiais Chefes de Polícia do Reino Unido (ACPO) propuseram um "Guia de Boas Práticas para evidências eletrônicas baseadas em Computador", que definem quatro grandes princípios para manipular evidências:

a) Primeiro Princípio – Nenhuma ação deve provocar a alteração de dados presentes em um computador ou em dispositivos de armazenamento, que serão submetidos a uma corte para julgamento.

b) Segundo Princípio - Em circunstâncias em que uma pessoa ache necessário acessar os dados originais guardados em um computador ou em uma mídia de armazenamento, essa pessoa deve ser competente para fazê-lo e deve ser capaz de prestar depoimento, explicando a importância e as implicações de suas ações.

---

[86] Procedimentos de Operação Padrão.
[87] ACPO, 1999, p. 10.
[88] Para obter maiores informações, acesse o site < http://www.swgde.org/ >

c) Terceiro Princípio - Uma trilha de auditoria ou outro registro de todas as atividades aplicadas às evidências eletrônicas devem ser criadas e preservadas. Um terceiro perito independente deve ser capaz de examinar os processos, repeti-los e obter o mesmo resultado.
d) Quarto Princípio - A pessoa responsável pela investigação é responsável por garantir que a lei e estes princípios sejam respeitados.

Marshall[89] assim sintetiza esses princípios:

a) Não modifique nada;
b) Se houver o risco de você modificar algo, tenha certeza do que está fazendo;
c) Registre tudo que você fez, na ordem correta;
d) Alguém deve ser responsável por garantir que tudo esteja sendo feito de forma legal e respeitando os princípios supracitados.

Com o objetivo de impedir a ocorrência de delitos, o autor defende que todas as medidas tomadas devem ser justificadas, apropriadas e proporcionais ao delito cometido.

Antes de iniciar qualquer trabalho, é essencial uma completa inspeção visual com a devida utilização de fotografias e anotação de tudo que for importante a fim de garantir que nenhuma informação seja perdida e todos os riscos sejam devidamente considerados.

Antes de iniciar a inspeção, torna-se necessário afastar qualquer pessoa do equipamento analisado, com o objetivo de impedir que qualquer prova seja plantada ou que as evidências sejam danificadas. Essa atividade é definida como ***Quarentena***.

Uma vez que o equipamento tenha sido colocado em quarentena, é necessário verificar se ele está funcionando. Assim, sua situação atual deve ser gravada usando fotografia, anotações ou quaisquer outros meios que descrevam exatamente o que pode ser visto.

Há opiniões diversas quanto à conexão a redes e comunicação on-line. Em geral, na ausência de um especialista, recomenda-se desconectar o equipamento analisado tão logo seja possível, mesmo antes de fazer uma fotografia da situação atual. Contudo, tal atitude apresenta alguns riscos, dentre eles: a interrupção abrupta da comunicação pode alertar os outros membros da gangue que algo anormal esteja acontecendo e isso pode levá-los a destruir evidências; é possível que o sistema detecte a perda de comunicação e inicialize, de forma automática, um processo de supressão de evidências; no caso de telefones celulares, a perda da comunicação pode levar a mudança de dados internos, o que pode, hipoteticamente,

atrapalhar as investigações. Em todo caso, o melhor caminho é procurar a consultoria de um especialista para saber o que fazer com o processo de comunicação on-line.

Com a exceção de dispositivos portáteis, recomenda-se que todos os dispositivos sejam desligados tão logo sejam apreendidos. Importante salientar que o processo de *shut down* NÃO seja feito de forma normal para garantir que os dados não sejam alterados. Deve-se, portanto, retirar o cabo de alimentação de energia diretamente do dispositivo analisado, permitindo, contudo, que sejam finalizadas as gravações em CD/DVD, bem como, as impressões, que produzem registros permanentes. Tão logo as tomadas tenham sido desconectadas, devem ser identificadas, caso precisem ser religadas. Tudo então deve ser empacotado e identificado para dar inicio à trilha de continuidade e auditoria de evidências. Todas as pessoas que receberem o material devem ser incluídas nos apontamentos do dispositivo.

Há um risco real de que qualquer interação com os dispositivos possa levar a alterações indevidas das informações presentes no dispositivo a ser analisado. Caso a situação do equipamento tenha sido alterada durante ou após a apreensão, isso pode indicar que alguém envolvido no manuseio do dispositivo tenha manipulado os dados.

Em geral, os objetos nem sempre são o que aparentam. Eles podem estar camuflados em outros objetos. Portanto, é importante checar acuradamente para identificar se todos os dispositivos digitais foram apreendidos. Além disso, é importante buscar todos os tipos de dados possíveis.

Além das considerações já feitas, importante compilação dos princípios e boas práticas na área de investigação forense foi feita na dissertação de mestrado de Reis e Geus. Dente elas, pode-se citar:

a) as ações tomadas durante a investigação forense não devem alterar as evidências;

b) qualquer ação que tenha o potencial de alterar, danificar ou destruir qualquer aspecto da evidência original deve ser conduzida por pessoa qualificada;

c) o investigador não deve confiar cegamente no sistema analisado, nem nos programas e arquivos nele encontrados;

d) cópias das evidências originais devem ser produzidas e, sempre que possível, a investigação deve ser conduzida sobre as cópias, que devem ser idênticas às evidências originais;

---

[89] MARSHALL,2008, p.

e) todas as evidências digitais coletadas, bem como as cópias produzidas devem ser autenticadas por meio de assinaturas criptográficas, permitindo a verificação de sua integridade;

f) toda evidência coletada deve ser identificada, contendo o número do caso investigado, uma breve descrição da evidência e a data e horário da coleta;

g) toda evidência coletada deve ser preservada em local de acesso controlado e livre de alterações;

h) todas as informações relativas à investigação devem ser documentadas de maneira permanente e devem estar disponíveis para revisão, permitindo, que outro investigador, a partir das informações documentadas, chegue às mesmas conclusões;

i) a cadeia de custódia das evidências coletadas deve ser mantida, documentando todas as informações relativas ao cuidado da evidência durante a sua análise;

j) as ferramentas usadas na investigação devem ser amplamente aceitas e testadas para garantir sua operação correta e confiável;

k) os procedimentos devem ser aceitos pela comunidade científica relevante ou suportados por demonstrações da precisão e confiabilidade das técnicas aplicadas;

l) os procedimentos devem ser revistos periodicamente para garantir sua contínua adaptabilidade e eficácia em relação às evoluções tecnológicas;

m) o investigador deve ser responsável pelos resultados da investigação e pelas evidências enquanto estiverem em sua posse;

n) o responsável pela investigação deve assegurar o rigoroso cumprimento dos procedimentos e protocolos estabelecidos.

8) Processo de Investigação Forense

O processo de investigação forense deve garantir a autenticidade e a integridade das evidências coletadas e dos resultados produzidos. Isso implica dizer que deve garantir que as informações obtidas estejam presentes nas evidências analisadas e não tenham sido alteradas ou contaminadas pelo processo de investigação. Devido ao alto grau de volatilidade das evidências digitais, isso é particularmente difícil. Portanto, torna-se essencial que se siga um método consoante a tecnologia envolvida.

Segundo Reis e Geus, “Toda informação relevante deve ser coletada para análise, e conforme as evidências digitais são encontradas, elas devem ser extraídas, restauradas quando necessário (evidências danificadas ou cifradas, por exemplo), documentadas e devidamente preservadas. Em seguida, as evidências encontradas podem ser correlacionadas, permitindo a reconstrução dos eventos relacionados ao ato ilícito. Muitas vezes a análise das evidências (correlação e reconstrução) resulta na descoberta de novas informações, formando um ciclo no processo de análise forense.” [90]

Assim, em um processo de análise forense de um sistema computacional[91] as seguintes atividades devem ser consideradas: coleta de informações; reconhecimento das evidências; coleta, restauração, documentação e preservação das evidências encontradas; correlação das evidências; e, reconstrução dos eventos.

Por óbvio, a tecnologia envolvida, as configurações do sistema em análise e as condições em que o sistema é encontrado interferem diretamente no processo investigativo. Mas, ainda que essas múltiplas variantes imponham restrições a esse processo, há uma linha mestra que deve respeitada na consecução de um processo de investigação forense. Assim, o framework geral do processo de investigação forense é o seguinte:

a) considerações e inteligência preliminares;
b) planejamento;
c) estabilização do sistema e decisões iniciais;
d) coleta, autenticação, documentação e preservação de material para análise;
e) análise.

Quanto melhor for definido o processo de análise forense, maiores serão as chances de sucesso. Assim, torna-se importante detalhar os procedimentos utilizados, bem como o uso de determinadas ferramentas e técnicas. Além disso, os princípios e boas práticas supracitados devem guiar o trabalho a ser executado para garantir o sucesso da investigação a ser realizada.

A primeira etapa do processo refere-se a ***considerações e inteligência preliminares***. Antes de iniciar a análise propriamente dita, deve-se considerar uma série de questões e fazer um trabalho inicial de inteligência. Assim, entender o problema, identificar as condições em que o sistema será entregue para investigação, conhecer as responsabilidades

[90] REIS & GEUS, 2001, p. 02.
[91] Idem, p. 02.

sobre cada parte do sistema e as relações de propriedade sobre as informações nele contidas, determinar se alguma lei ou direito individual poderá ser violado, determinar as restrições impostas à investigação e delimitar o alvo da investigação são objetos dessa primeira etapa.

Com base nessas informações, a investigação poderá ser então planejada. Assim, definir as atividades que serão realizadas, bem como, preparar um conjunto de ferramentas e o sistema de análise com a configuração de hardware e software mais adequada são objetivos da fase de ***planejamento***.

Com o objetivo de preservar o máximo de evidências e proteger os sistemas e dados fora do escopo da investigação, surge a etapa de **estabilização do sistema e decisões iniciais**. Nesse caso, são tomadas nessa etapa decisões relativas ao método de coleta de informações mais adequado, à necessidade de coleta de dados voláteis, ao método de desligamento do sistema, à necessidade de coleta de tráfego de rede e possibilidade de rastreamento do atacante e à necessidade de remoção do sistema para um ambiente controlado de análise.

Uma decisão importante nesta etapa refere-se ao desligamento do sistema, que pode ou não ser efetuado, a critério do investigador. Alguns defendem que o desligamento pelo cabo de energia, com a conseqüente perda de informações voláteis é a melhor opção para congelar o sistema em seu estado corrente. Além disso, alegam que a manutenção do sistema em funcionamento ou o seu desligamento administrativo normal podem expô-lo a armadilhas que destroem rastros ou à alteração ou remoção de arquivos como parte do procedimento normal de desligamento.

A corrente contrária defende que o desligamento imediato antes da coleta de informações voláteis resulta na perda de importantes vestígios referentes às atividades em execução. Em ambos os casos, é importante que nenhuma atividade de investigação utilize os programas existentes no sistema em análise, uma vez que esses executáveis podem ter sido alterados pelos suspeitos com o fito de modificar as informações a serem analisadas. Diante do exposto, a decisão quanto ao desligamento do sistema deve ser tomada pelo investigador com base nas situações particulares da investigação em andamento.

As decisões tomadas nessa etapa do processo de investigação impactarão a escolha do método a ser utilizado para a ***coleta e análise das informações do sistema***

suspeito. A tabela abaixo, apresentada por Reis e Geus[92], apresenta a relação entre o método de coleta e análise e o nível de esforço empregado para proteger as evidências e evitar a execução de código hostil.

Tabela III – Relação entre o método de coleta e análise e o nível de esforço empregado para proteger as evidências e evitar a execução de código hostil. (íntegra de Reis e Geus, pág. 58)

Método	**Vantagens**	**Desvantagens**
Usar uma estação forense dedicada para examinar o disco suspeito (protegido contra escrita) ou uma imagem do mesmo	Não requer preocupação quanto à validade do software ou hardware da máquina suspeita	Pode depender do desligamento do sistema suspeito. Pode resultar na perda de informações voláteis.
Inicializar a máquina comprometida usando um Kernel e ferramentas verificados e protegidos contra escrita, contidos em uma mídia removível.	Conveniente e rápido. Nesse caso, os discos da máquina suspeita devem ser montados somente para leitura.	Assume que o hardware da máquina suspeita não foi comprometido. Resulta na interrupção dos serviços disponibilizados pelo sistema suspeito e pode causar a perda de informações voláteis.
Reconstruir o sistema suspeito a partir de sua imagem e, então, examiná-lo.	Recria completamente o ambiente operacional do sistema suspeito, sem o risco de alterar as informações originais.	Requer disponibilidade de hardware idêntico ao do sistema suspeito. Pode resultar na perda de informações voláteis.
Examinar o sistema suspeito através de mídias removíveis contendo ferramentas verificadas.	Conveniente e rápido. Permite acessar informações voláteis.	Se o Kernel estiver comprometido, os resultados podem ser inconsistentes.
Verificar o software contido no sistema suspeito e, então, utilizá-lo para conduzir o exame.	Requer uma preparação mínima. Permite acessar informações voláteis e pode ser realizado remotamente.	Pode tomar muito tempo e o programa usado para verificação de integridade pode estar comprometido. A falta de proteção contra escrita nos discos do sistema suspeito pode resultar na alteração ou destruição de informações.
Examinar o sistema suspeito usando o software nele contido, sem qualquer verificação.	Requer nenhuma preparação. Permite acessar informações voláteis e pode ser realizado remotamente.	Método menos confiável e representa exatamente aquilo que os atacantes esperam que seja feito. Na maioria das vezes, é uma completa perda de tempo.

A etapa de **Coleta, autenticação, documentação e preservação de material para análise** é a mais importante de todo processo de investigação. Essa etapa, se conduzida de forma inadequada, pode comprometer toda a investigação forense. Os dois grandes perigos, que devem ser evitados a todo custo, são a perda e a alteração do material de análise. Assim, os autores defendem que toda informação deve ser tratada como se fosse utilizada para fins judiciais. Além disso, respeitando a ordem de volatilidade, deve ser coletada a maior

[92] REIS & GEUS , 2001, p. 58.

quantidade possível de evidências. Cada item coletado deve ser autenticado, identificado, catalogado e preservado. Por fim, devem ser produzidas cópias exatas e autenticadas das informações digitais coletadas.

Na etapa de coleta de material para análise, uma das atividades mais importantes é a documentação dos itens coletados. Cada item deve ser identificado unicamente e seu estado original deve ser bem detalhado. Essa descrição deve conter a localização original, data e hora da coleta e a identificação da pessoa responsável. O transporte e o armazenamento devem ser feitos de forma cuidadosa, mantendo a integridade dos mesmos.

O guia de boas práticas para evidências eletrônicas requer que o exame dos dispositivos digitais seja feito de forma a minimizar a possibilidade de contaminação digital. Isso implica dizer que ainda que não seja possível, todo trabalho deveria ser feito sobre uma cópia do dispositivo ao invés do original. Isso nem sempre é possível, como em computadores compartilhados ou em redes.

A autenticidade e a integridade das informações digitais coletadas podem ser estabelecidas por meio de assinaturas criptográficas, como o MD5 e o SHA. É possível determinar a autenticidade de uma informação digital coletada por meio da simples comparação entre o seu hash criptográfico com a assinatura criptográfica da informação original. No caso de informações voláteis ou quando o sistema suspeito não pôde ser desligado não é possível fazer essa comparação.

O procedimento básico para a coleta de informações digitais de um sistema suspeito é o seguinte: coletar as informações voláteis, desligar a máquina suspeita, instalar o disco da máquina suspeita no sistema de análise e produzir sua imagem.

Para que a coleta de informações voláteis seja possível, é necessário que o sistema esteja em funcionamento. Assim, torna-se fundamental não utilizar os programas presentes no sistema suspeito e não escrever no disco da máquina analisada. Para tanto, pode-se utilizar um conjunto de ferramentas confiáveis, residentes em alguma mídia removível, montada na máquina suspeita, e o resultado da análise também deve ser redirecionado para uma mídia removível ou para a rede. É durante esse processo de extração que é gerada uma assinatura criptográfica na estação forense com o objetivo de provar a integridade dos dados armazenados na máquina de análise. Devido à alta volatilidade dessas informações, a geração do hash criptográfico dos dados enviados para a estação forense deve ser feita no momento em que as informações são coletadas.

Como essa primeira etapa requer um exame direto dos dispositivos suspeitos, envolve um significante risco de infringir o primeiro princípio do ACPO. Contudo, uma correta aplicação dos demais princípios propicia uma maior proteção na etapa de coleta de evidências. A visualização das evidências pode ser feita de forma off-line ou on-line.

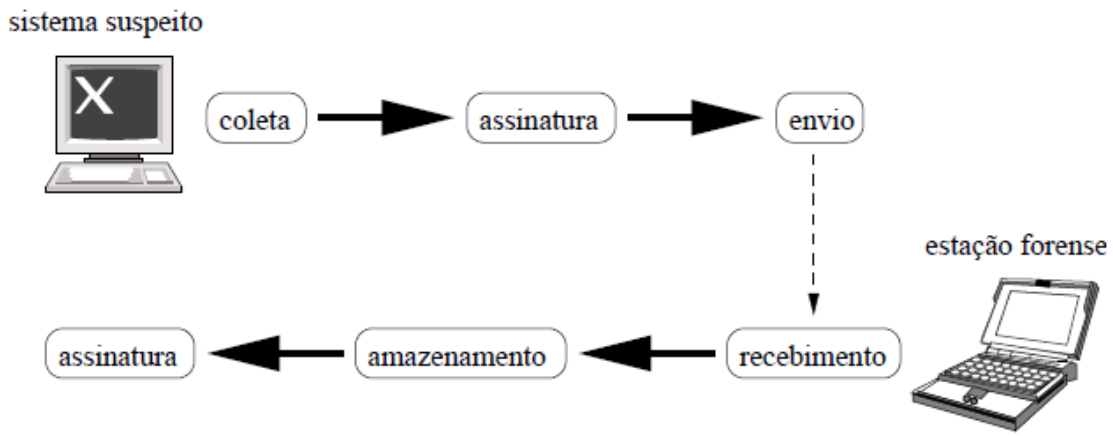
Em uma situação típica, o dispositivo será analisado em um estado off-line, ou seja, terá sido desconectado da rede e desligado para permitir que o perito remova todas as conexões e faça uma análise mais confiável. Idealmente, os dispositivos serão conectados a partir de um dispositivo anti-gravação (write-blocking) para que não sejam feitas contaminações acidentais.

Nesse caso são utilizados métodos físicos para garantir que as evidências possíveis não sejam contaminadas. A grande desvantagem nesse caso é a necessidade de desligar o dispositivo, o que nem sempre é possível.

No caso da análise em equipamentos on-line, essa é a atividade mais arriscada que um perito pode realizar. Há algumas ferramentas confiáveis que permitem o acesso a mídias read-only tais como CDs. De acordo com Marshall, é difícil utilizar as evidências adquiridas neste formato por elas conterem um alto grau de incerteza. Contudo, as informações obtidas podem ser utilizadas com o propósito de formar um conhecimento sobre o assunto (inteligência).

A figura abaixo, proposta por Reis e Geus, bem define o fluxo de coleta de informações voláteis no sistema suspeito até seu armazenamento na estação forense.

Fluxo das informações voláteis desde a coleta no sistema suspeito até seu armazenamento na estação forense (Reis e Geus, p. 60)



A produção da ***imagem*** do sistema analisado é uma das etapas mais críticas do trabalho investigativo. O primeiro princípio estabelecido pela Associação de Oficiais Chefes de Polícia do Reino Unido (ACPO) [93], publicado no Guia de Boas Práticas para evidências eletrônicas baseadas no computador, dispõe que nenhuma ação investigativa deve modificar dados presentes na máquina ou nas mídias de armazenamento que poderão ser utilizadas como prova diante de um tribunal. Isso implica dizer que toda ação deve ser feita sobre uma cópia do material analisado, buscando, assim, preservar o original.

Diante disso, para gerar uma imagem que possa ser analisada como se fosse o disco original, pode-se utilizar uma ferramenta que crie um arquivo de imagem contendo todo o fluxo de bits lido do disco suspeito, sem qualquer alteração na ordem ou no conteúdo, ou fazer um espelhamento do disco suspeito em outro disco de capacidade similar ou maior. Como essa cópia deve conter cada bit do disco de origem, programas normais de cópia ou backup não são apropriados por copiarem apenas os dados reconhecidos pelo sistema de arquivos. Existem diversos aplicativos disponíveis no mercado, inclusive equipamentos especiais destinados a tal finalidade, tal como o Image MaSSter Solo Forensic Unit[94]. O procedimento mais comum é a instalação do disco suspeito na estação forense, onde a imagem é produzida e armazenada em um arquivo. Recomenda-se a adoção de nomes que identifiquem com precisão o disco copiado. A adoção de assinaturas criptográficas serve para garantir que os dados tenham sido copiados com exatidão. Assim, as assinaturas do disco suspeito e de sua imagem devem ser idênticas.

Outra observação importante refere-se à "***esterilização***" do disco destino. Antes de efetuar o espelhamento do disco suspeito, é imprescindível eliminar qualquer informação que possa ser confundida com os dados do disco suspeito. Assim, deve ser feita uma limpeza do disco destino e uma verificação para garantir que ele esteja apto ao processo de geração da imagem.

Deve-se, portanto, produzir uma cópia fiel do dispositivo original, incluindo todos os espaços não usados, os dados apagados e, se possível, as áreas corrompidas. Existem ferramentas especiais para a execução dessa atividade. A geração de imagem off-line é a forma mais simples de fazer a cópia. Nesse caso, o equipamento é conectado à estação que

[93] ACPO, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf
[94] Para obter mais informações, acesse o site http://www.ics-iq.com/ .

fará a cópia usando o dispositivo anti-gravação e por meio de ferramenta própria, a cópia será feita. Uma vez que a cópia seja feita, ela será utilizada e o original será preservado.

Sempre que não for possível desligar o sistema suspeito, a imagem será feita on-line com ferramentas adequadas. Contudo, há problemas de incerteza e imprecisão de informação, o que pode ser mitigado com ferramentas adequadas.

Objetivo principal do processo de investigação forense, a etapa de ***análise*** tem como objetivo examinar todo material coletado em busca de evidências. É importante investigar todas as fontes de informação do sistema suspeito, buscando elementos anormais e indevidos.

Backups podem ser utilizados na fase de análise, mas eles representam apenas uma parte da informação passada. Para compreender melhor a situação, vários backups deverão ser analisados em conjunto.

Uma vez que a imagem tenha sido gerada, a imagem e o dispositivo devem ser tratados como se fossem cenas de um crime, com todo cuidado para preservar a contaminação e a alteração das evidências.

Além do método anti-gravação, outros processos podem ser utilizados para garantir que o processo utilizado pelo perito não contenha efeitos adversos tanto no original quanto na imagem utilizada. Esses métodos podem ser usados para alertar sobre mudanças acidentais, permitindo, assim, a re-análise de pontos problemáticos.

Algoritmos de Hashing são usados para gerar “assinaturas” digitais que são únicas para determinadas porções de dados. Os valores calculados para os dados originais devem ser iguais àqueles calculados para as cópias. Qualquer diferença detectada leva à suspeição dos dados sob análise.

A modificação de um único bit leva a uma “assinatura digital” completamente diversa da original. Há excelentes ferramentas disponíveis que podem ser utilizadas com esse propósito, assegurando, assim, a integridade das evidências. Além disso, há outras ferramentas que permitem registrar um histórico de atividades executadas sobre as evidências durante a análise.

Quanto à localização das evidências, há basicamente quatro tipos de dados ou arquivos que devem ser considerados:

a) Dados “vivos” – Representam os dados presentes em um formato que podem ser acessados pelo usuário ou por um software normal. São geralmente os dados que apresentam as

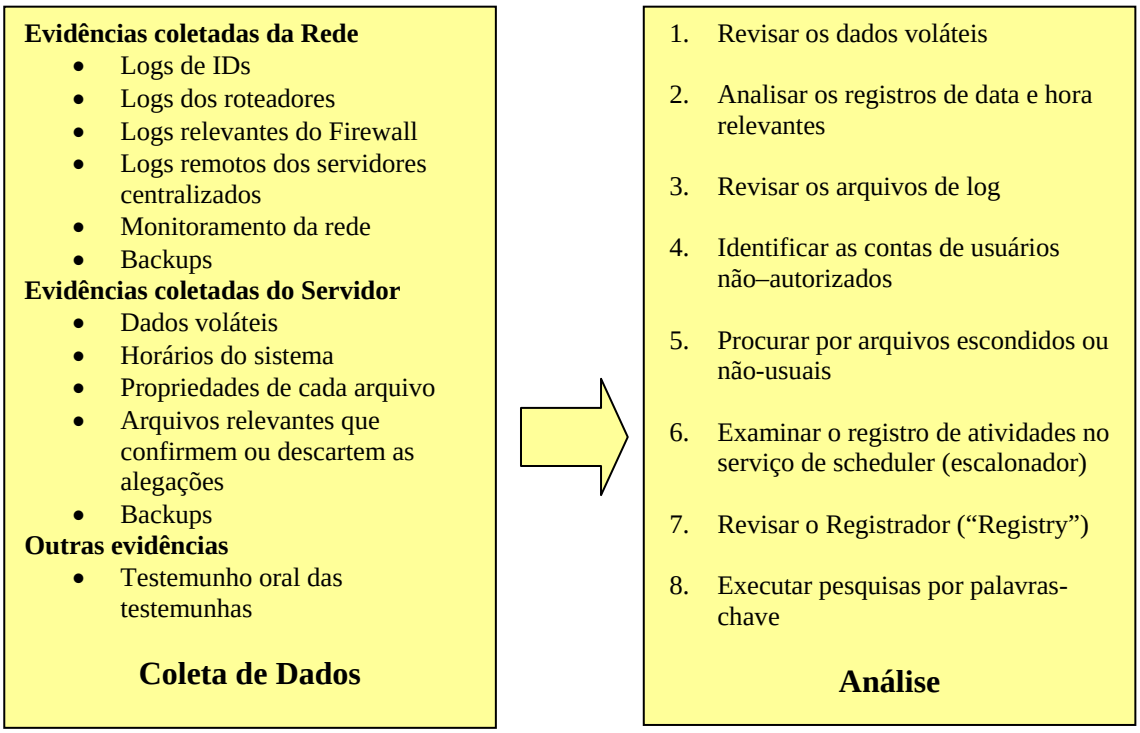
melhores evidências. Em geral, apresentam informações quanto à data e hora de atualização, criação e acesso.

b) Dados deletados – Também de grande representatividade como evidências, apresentam dados que o usuário ou o sistema operacional decidiu eliminar do sistema por algum motivo. Apesar de não terem o mesmo grau de confiabilidade dos dados "vivos", também podem ser usados. Além disso, há ferramentas que recuperam essas informações.

c) Área de swap – A área de swap é utilizada pelo computador como uma extensão da memória RAM e nele é possível encontrar dados não gravados nos dispositivos de armazenamento. É uma boa fonte de informação para senhas de arquivos encriptados ou outros dados sensíveis.

d) Áreas demarcadas – Refere-se a dados armazenados ao lado de dados vivos, mas que não foram gravados intencionalmente pelos usuários. Relaciona-se à unidade de alocação mínima definida no computador. Quando há alguma sobra, o sistema utiliza para gravar informações que estão presentes na memória principal. Isso pode levar à detecção de evidências.

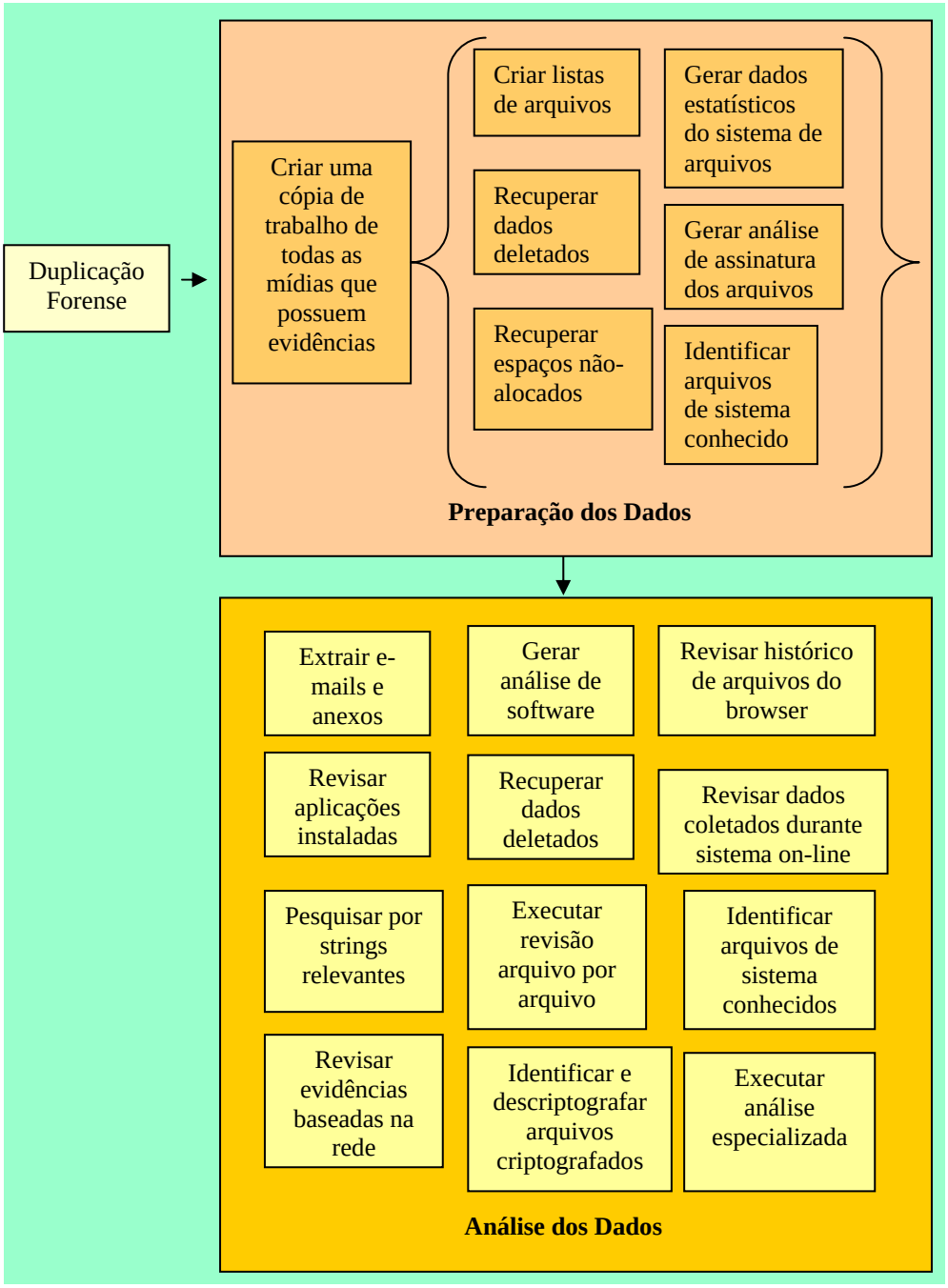
O quadro[95] abaixo resume bem as atividades que são executadas nas fases mais importantes do processo de investigação forense:



Síntese das atividades de coleta de dados e análise (PROSISE, 2003, p. 26)

[95] PROSISE, 2003, p. 26.

A análise forense inclui a revisão de todos os dados coletados, ou seja, dos logs, arquivos, arquivos de configuração do sistema, histórico de navegação na internet, mensagens de e-mails, aplicações instaladas e arquivos gráficos. Além disso, há que se fazer a análise de softwares instalados e do registro da data e hora dos arquivos, executar pesquisas por palavras chave e quaisquer outras ações necessárias à investigação. O quadro abaixo resume o que pode ser feito durante o processo de análise forense[96]:



[96] PROSISE, 2003, p. 29.

Por fim, a atualização da cadeia de custódia e a documentação das tarefas executadas e evidências encontradas são atividades rotineiras na etapa de análise. Com base nesse resultado, será gerado um laudo pericial, que poderá auxiliar na formação da convicção do juiz.

O laudo pericial representa a materialização da prova pericial. Portanto todo laudo pericial deve ser feito com qualidade, pois contribui para a formação da convicção do juiz. Para tanto, deve ser claro, objetivo e conciso, abstendo-se de julgamentos com bases pessoais do perito e deve conter a fundamentação e a conclusão as quais o perito chegou. Deve primar pelo rigor tecnológico, atendo-se, portanto, a sua área de conhecimento. Além disso, deve apresentar os documentos, evidências e meios necessários à formação da convicção do juiz. Caso não seja claro, o artigo 438 do CPC permite que seja realizada segunda perícia, quando possíveis omissões ou inexatidão poderão ser saneadas.

Quando se pensa em provas, pensa-se na relação entre os vestígios. Essa relação deve ser demonstrada de forma exata no laudo pericial, que deve apontar a extensão e a causa do fato, indicando se houve negligência, imprudência, imperícia ou dolo, por exemplo[97].

[97] ZOCHIO , 2010, p. 49.

9) Considerações finais

Ao longo do presente trabalho, estudamos o processo de investigação forense como forma de garantir a autenticidade e a integridade das evidências coletadas e dos resultados obtidos. Vimos os princípios que devem ser respeitados e a ordem de volatilidade das evidências a serem analisadas. Ainda que o processo e os princípios tenham sido respeitados integralmente, como garantir que as informações não tenham sido plantadas antes mesmo de efetuar a cópia sobre o dispositivo original?

Sabe-se que o sistema de arquivos, fonte de informação vital para a análise forense, pode ser alterado por um especialista da área. Não falta literatura para nos apontar como fazer essas modificações. Como então garantir a integridade da prova e seu valor probatório em processos criminais, afastando uma acusação "injusta" de prova plantada em um contraditório judicial?

A maior parte das perícias relacionadas a ilícitos penais e civis condiciona-se ao exame de determinados locais e à coleta e posterior análise das evidências materiais identificadas. As evidências que demandam exames laboratoriais só podem ser admitidas como meios de prova se a coleta, o manuseio e a análise respeitarem aos procedimentos determinados com o fito de garantir a integridade do material a ser examinado e a idoneidade dos meios empregados. Muitas vezes, a qualidade dessas evidências depende do processo de coleta e de armazenagem até a chegada nos laboratórios de análise[98].

É por essa razão que todo procedimento realizado entre a comunicação do fato à autoridade competente e a requisição da perícia deve obedecer a um rigoroso sistema de controle denominado de ***Cadeia de Custódia***. Esse é o calcanhar de Aquiles de todo o processo. Ou seja, a garantia de integridade da prova, seja digital ou convencional, é obtida pela manutenção da cadeia de custódia.

De forma mais genérica, a Cadeia de Custódia:

[98] DEL CAMPO, 2008, p.235.

> *"É usada para manter e documentar a história cronológica da evidência, para rastrear a posse e o manuseio da amostra a partir do preparo do recipiente coletor, da coleta, do transporte, do recebimento, do armazenamento e da análise, portanto, refere-se ao tempo em curso no qual a amostra está manuseada e inclui todas as pessoas que a manuseiam. Esta terminologia vem sendo legalmente utilizada para garantir a identidade e integridade da amostra, em todas as etapas do processo.*[99]"

Assim, Cadeia de Custódia pode ser definida como um conjunto de procedimentos administrativos que certificam a preservação e a integridade das evidências coletadas durante todas as etapas do processo investigativo, de forma a garantir a confiabilidade dos resultados obtidos. Ela requer que seja possível rastrear a localização da evidência do momento em que foi coletada até o momento em que for apresentada diante de uma corte judicial[100].

Com o fito de atender aos requerimentos da cadeia de custódia, alguns departamentos de polícia têm locais próprios para armazenar as evidências em um ambiente seguro. Especialistas e oficiais de justiça devem registrar qualquer entrada ou saída da evidência desse ambiente.

Uma vez que podem se passar anos entre a coleta das evidências e o julgamento do crime, outro grande desafio é garantir que os dados apresentados na corte sejam iguais aos coletados no local do crime. Uma saída já discutida no trabalho é que os *hashes* MD5 dos dispositivos originais sejam iguais aos gerados para as mídias duplicadas. Além disso, para cada arquivo em análise deve ser gerado um arquivo *hash* MD5.

Em suma, deve-se atentar para os seguintes procedimentos:

a) ao se examinar um disco rígido em um computador, deve-se gravar informações sobre o sistema de computador examinado;

b) deve-se tirar fotografias digitais do sistema original e/ou das mídias que estão sendo duplicadas;

c) deve-se preencher uma etiqueta de evidência para a mídia original e para as mídias duplicadas;

d) deve-se rotular todas as mídias apropriadamente com uma etiqueta de evidência;

e) dever-se armazenar todas as cópias das evidências em um cofre de evidências;

f) o depositário da evidência deve fazer um histórico de registro das evidências;

g) todas os exames devem ser feitos na cópia da evidência;

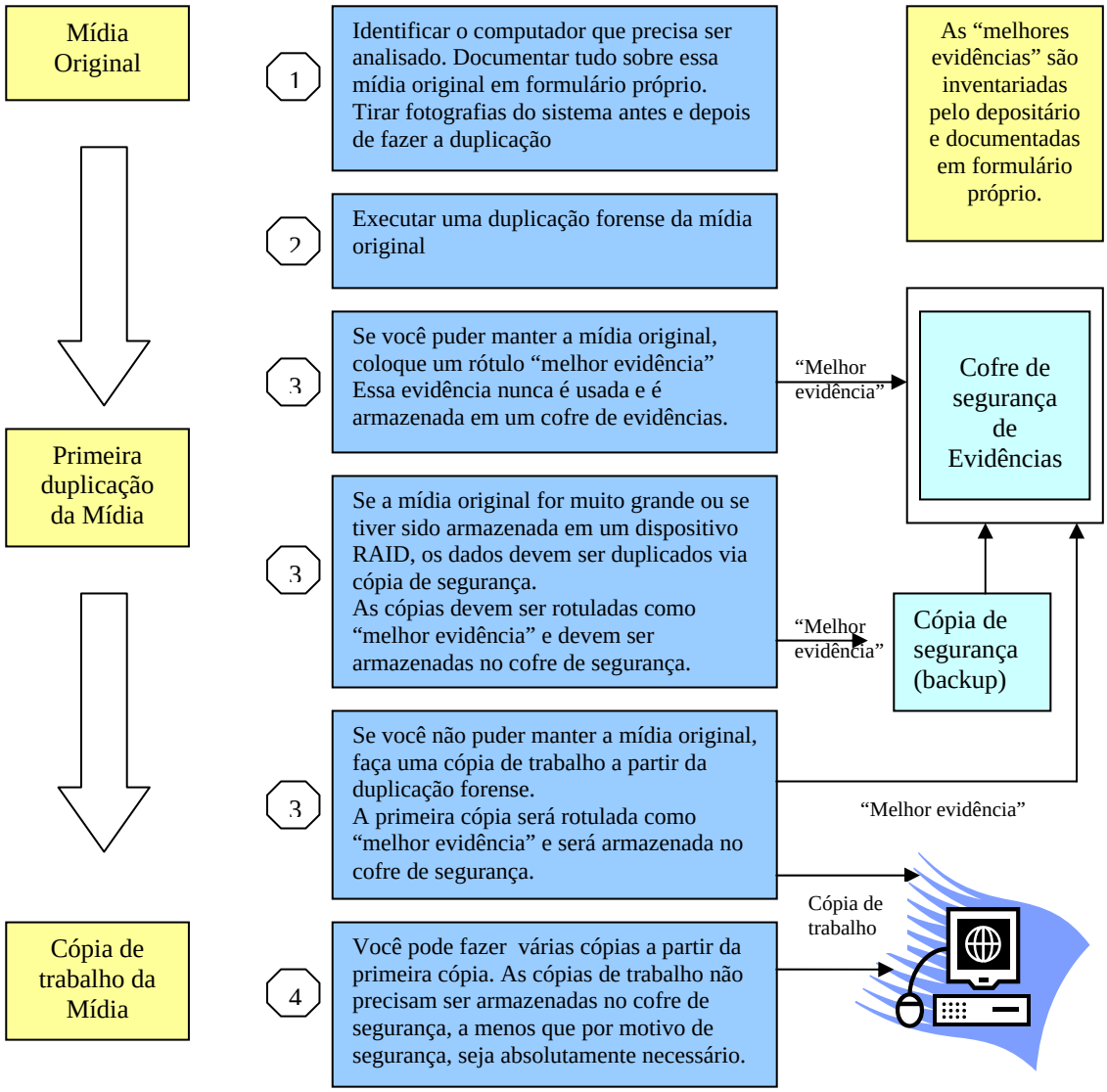
---

[99] LOPES, 2007, p. 2.
[100] PROSISE, 2003, p. 200.

h) o depositário deve garantir que sejam feitas cópias de segurança das evidências identificadas;

i) o depositário deve ser responsável por executar auditorias periódicas para garantir que as evidências estejam armazenadas de forma adequada e etiquetadas.

A figura abaixo sintetiza o processo de manipulação de evidências em uma cadeia de custódia[101]:



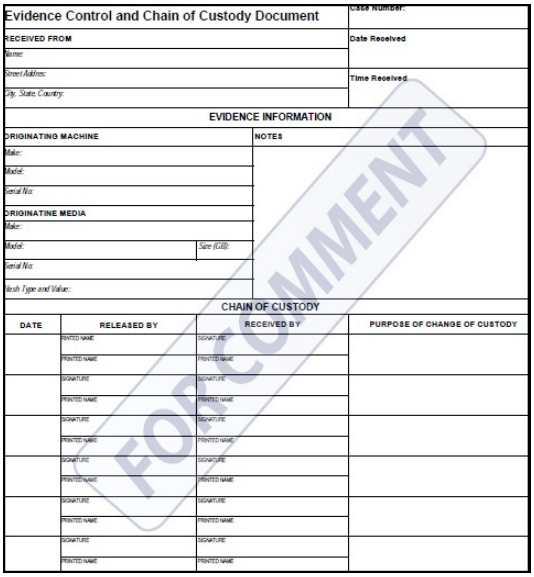
Processo de Manipulação de Evidências (PROSISE, 2003, p. 204)

[101] PROSISE, 2003, p. 204.

Depois de registrar esses detalhes do sistema, devem-se tirar várias fotografias das evidências como forma de assegurar sua situação real, bem como, capturar sua configuração corrente. Uma cadeia de custódia apropriada deve conter o histórico de toda a manipulação ocorrida com a evidência, assim deve conter o local onde a evidência foi coletada, quando foi coletada, quem entregou a evidência para especialista em computação forense, dados sobre o equipamento e a mídia onde estava armazenada a evidência original, como foi feita imagem forense e o histórico de mudanças na custódia da evidência.

Ou seja, antes que as evidências eletrônicas sejam reunidas, certas informações devem ser registradas, dentre elas: as pessoas que ocuparam e que acessaram o escritório quando as evidências originais foram encontradas; os usuários que usavam o sistema; a localização do computador ou dos dispositivos digitais na sala; a situação do sistema (ligado ou desligado); a data/hora do sistema BIOS; as conexões de rede; as pessoas presentes durante a duplicação forense; os números de série, os modelos e marcas dos dispositivos digitais e seus componentes; e os periféricos conectados ao sistema.

Para tanto, um formulário de cadeia de custódia deve acompanhar a evidência desde o momento da coleta até o seu descarte, quando não for mais necessária. Uma sugestão de formulário[102] encontrado na internet:



Evidence Control and Chain of Custody Document

Case Number:

RECEIVED FROM

Name:

Street Address:

City, State, Country:

Date Received

Time Received

EVIDENCE INFORMATION

ORIGINATING MACHINE

Make:

Model:

Serial No:

NOTES

ORIGINATINE MEDIA

Make:

Model:

Size (GB):

Serial No:

Hash Type and Value:

CHAIN OF CUSTODY

DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
	PRINTED NAME / SIGNATURE	PRINTED NAME / SIGNATURE	
	PRINTED NAME / SIGNATURE	PRINTED NAME / SIGNATURE	
	PRINTED NAME / SIGNATURE	PRINTED NAME / SIGNATURE	
	PRINTED NAME / SIGNATURE	PRINTED NAME / SIGNATURE	
	PRINTED NAME / SIGNATURE	PRINTED NAME / SIGNATURE	
	PRINTED NAME / SIGNATURE	PRINTED NAME / SIGNATURE	

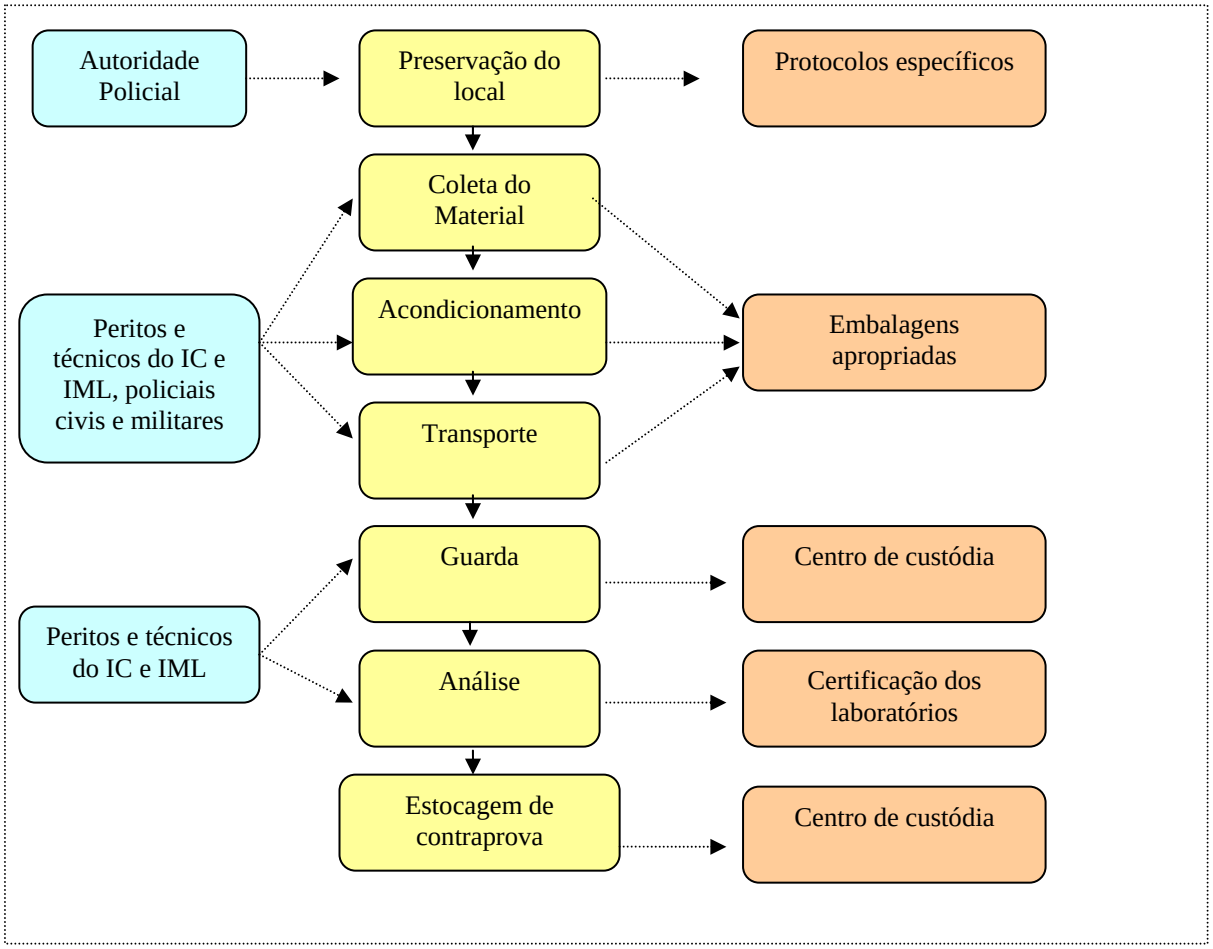
FOR COMMENT

Exemplo de formulário para registrar a Cadeia de Custódia

[102] http://blog.prenato.com/2010/03/onde-deveria-comecar-em-uma.html . Acessado em 28 de junho de 2011.

Observe que há campos para registrar todas as informações supra mencionadas. Além disso, a assinatura digital ou hash da imagem (MD5 e SHA-1), bem como os procedimentos utilizados para realizar a coleta da evidência, como softwares, write blockers e formato da imagem, devem ser registrados. Além do preenchimento do formulário acima, recomenda-se que seja feita ata notarial no momento de coleta dos dados.

Existem, portanto, cuidados e princípios gerais que podem ser elencados visando dar uma maior confiabilidade à perícia. Esses procedimentos têm como objetivo padronizar o manuseio das evidências, minimizar a possibilidade de extravio e dados, e permitir a identificação e responsabilização das pessoas envolvidas. O quadro abaixo apresenta as principais etapas de uma cadeia genérica de custódia[103] para provas periciais:



Cadeia Genérica de Custódia (DEL CAMPO, 2008, p. 235)

[103] DEL CAMPO, 2008, p. 235.

A garantia da integridade da prova, seja digital ou convencional, é obtida, portanto, pela manutenção da cadeia de custódia, que é responsável por gerar e manter os registros referentes a toda manipulação e guarda das provas. Ademais, a tecnologia envolvida no suporte ao arquivo digital permite agregar garantias de manutenção ou detecção da violação da integridade da prova, e desta forma chega-se a um resultado ainda mais robusto.

Em alguns casos, dadas as características da prova digital e as tecnologias disponíveis em complemento à cadeia de custódia, pode-se agregar mais algumas garantias de não forjabilidade e manutenção de integridade. Quando da cópia segura da imagem, podem ser usados resumos criptográficos. Se a mídia original for travada como apenas para leitura, sendo adicionados lacres e os hashes forem mantidos em um CD ou DVD ROM, a probabilidade de adulteração - forja ou plantação de prova - é muito reduzida, mantida a cadeia de custódia.

Outro exemplo é o uso de hashes para procurar arquivos em uma imagem sob análise sem disponibilizar ao perito o arquivo original. Novamente a probabilidade de alteração é muito baixa.

Suponha que se deseje plantar ou forjar uma prova e já se tendo um arquivo para isto. Pode-se ou plantar como um arquivo, possivelmente deletado, forjando-se os metadados referentes às estruturas de dados do sistema de arquivo, ou plantar como uma stream de bits sem os metadados. Apesar de a segunda opção ser mais simples, as duas requerem grande expertise, compatível com o de um perito experiente e acesso físico à mídia original, suas cópias seguras e os hashes. Ou seja, o conhecimento técnico não seria condição suficiente para a adulteração, mas o acesso físico à mídia. Em outras palavras, seria necessário quebrar a cadeia de custódia.

Portanto, o valor probatório recai sobre os mesmos requisitos da prova convencional, ou seja, a manutenção da cadeia de custódia e a qualidade da análise dos indícios.

Ocorre que, se por um lado, apesar de ser possível alterar os dados presentes nos dispositivos, por outro, pelo princípio de Locard, é impossível apagar todos os rastros dessa atividade. O princípio fundamental da Ciência Forense é conhecido como ***Princípio de Intercâmbio*** ou ***Princípio de Locard*** que estabelece que quando um indivíduo entra em contato com um objeto ou outro indivíduo, sempre deixa vestígio desse contato. Não há como eliminar todos os rastros.

Nesse cenário, caso o juiz considere o laudo impreciso, pode solicitar segunda perícia, o que permitirá, por meio da análise dos formulários de registro da cadeia de custódia e do material mantido no cofre de segurança, identificar o histórico de modificações ocorrido nas evidências detectadas. Mais uma vez, percebe-se que o valor probatório dos arquivos digitais foi mantido, estabelecendo, assim, o seu valor legal.

CONCLUSÃO

A adesão maciça dos usuários às redes mundiais, o substancial aumento de processamento dos computadores modernos e a expansão do uso de comunicação sem fio provocaram uma grande revolução na sociedade em que vivemos. Formamos uma sociedade absolutamente dependente da tecnologia digital. O que hoje se observa é que as transações comerciais e os negócios jurídicos, antes consolidados basicamente pelo papel, estão sendo feitos por meio de documentos digitais. Intermináveis são os exemplos dessa utilização no dia-a-dia: recibo de pagamento, ingresso, inscrição para concurso público, dentre outros. Mesmo na esfera jurídica, a adoção de arquivos digitais também já é uma realidade.

O resultado é que tanto cidadãos de bem quanto criminosos tem igual acesso à tecnologia e dela se utilizam para realizar suas atividades. O uso de computadores em práticas criminosas tem se tornado cada vez mais comum. Além dos crimes tradicionais, roubo, estelionato, extorsão e tráfico de drogas, surgiu uma nova classe de crimes, os "crimes da internet", tais como a difamação e a violação de sites, o ataque a servidores, a disseminação de falsos e-mails, o roubo de dados ("phishing scan"), a disseminação de vírus de computador, as retiradas e transferências de contas bancárias, dentre outros.

Essa realidade demanda um conhecimento técnico cada vez maior na identificação de evidências e aumenta o grau de importância da Informática na comprovação de seu valor probatório na Justiça. Entende-se por evidência digital qualquer informação armazenada ou transmitida no formato digital, seja pedaço de dado ou software, que tenha algum significado relevante para a investigação. Portanto, o que antes era comprovado por papel, passa a ser feito por arquivo digital.

Ocorre que existem duas classes de arquivos, aqueles que atestam sua integridade e autenticidade por meio da adoção de assinatura digital e o restante, que não utiliza qualquer mecanismo de garantia. Cabe ressaltar que esse "restante" corresponde à grande maioria dos documentos que trafegam em meio digital.

Diante desse cenário, vários questionamentos foram colocados como objeto de estudo do presente trabalho. Dentre eles, é possível usar esses arquivos como prova? Se a autoria é um aspecto fundamental na prova documental, como garanti-la em documentos que

se encontrem em meio magnético? Como atestar a autenticidade e integridade desses arquivos que correspondem a mais de noventa por cento dos documentos gerados atualmente, sem comprometer o devido processo legal? Como garantir que esses documentos não tenham sido violados ou não sejam provas plantadas? Como essas novas tecnologias podem nos auxiliar a responder a essas perguntas?

Na elucidação de um crime e diante de uma sociedade cada vez mais dependente de tecnologia, tornou-se comum, portanto, considerar se há algum dispositivo digital que contenha informações relacionadas aos crimes cometidos. Ainda que não tenha havido uma participação direta na cena do crime, seu uso por um dos envolvidos pode agregar importantes informações para sua elucidação. Assim, o arquivo digital residente na memória de um computador ou em memórias auxiliares pode e deve ser utilizado pela parte interessada em um processo como forma de influir na cognição do juízo.

Quanto à convicção do juiz, o sistema probatório brasileiro baseia-se no princípio da livre apreciação das provas pelo juiz. Nesse sentido, tanto o Código de Processo Penal como o Código de Processo Civil seguem a mesma linha, e dispõe que o juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação. Há entendimento pacífico de que todo documento poderá ser utilizado como prova desde que seja apresentado inteiro, completo, sem qualquer vestígio de alteração ou mutilação; e, respeite sua forma obrigatória, sob pena de nulidade.

Ao observar a pirâmide informacional proposta por Urdaneta, percebe-se que os documentos compõem as camadas mais inferiores, sejam elas, relacionadas a dados, de onde se pode extrair a informação. Mas, essas camadas são apenas o suporte informacional disponibilizado aos magistrados para que possam formar a sua convicção. Assim, a compreensão dessa informação compõe a estrutura informacional de mais alto nível responsável pelo resultado de seus julgados.

A prova é, portanto, considerada como a base de argumentação para formar a convicção do juiz. No processo criminal, por serem mais restritas do que nos demais processos, as provas assumem uma relevância ainda maior, uma vez que é por meio dela que se busca a verdade manifesta dos fatos, que podem ou não levar à imposição de restrições à liberdade.

Todos os meios de prova podem ser utilizados para auxiliar a formação da convicção do juiz. No processo criminal, contudo, a confissão só motiva uma condenação se o juiz tiver absoluta certeza da autoria do crime. Para admitir uma acusação, o juiz deve estar convicto de sua veracidade, bastando apenas uma dúvida quanto à culpabilidade, para que a condenação seja obstada. Rege o princípio *in dúbio pro réu* que todo caso duvidoso seja interpretado a favor do acusado.

Assim, pelo princípio da livre convicção, o juiz pode aplicar os referidos diplomas legais para fundamentar a utilização dos documentos eletrônicos apresentados em sua sentença sempre que estiver convicto da autenticidade e integridade desses documentos.

A previsão legal para os meios de prova é exemplificativa, sendo admitidas as provas não previstas expressamente na legislação. Por outro lado, são inadmissíveis as provas que ferem os princípios de respeito ao direito de defesa e à dignidade humana. A grande preocupação é não permitir a condenação de um inocente, mas garantir que os criminosos paguem pelos seus erros, sob pena de causar uma comoção social e um estímulo ao desrespeito às leis.

Portanto, a análise cuidadosa das provas é essencial para garantir a harmonia social. Nesse cenário, a utilização de arquivos digitais como prova pode promover a realização da justiça. Contudo, para que um arquivo digital tenha força probante é necessário garantir sua autenticidade e sua integridade.

Em ordenamento jurídico brasileiro, o projeto de lei 4.906/2001 já reconhece a criptografia assimétrica como instrumento de garantia de autoria e autenticidade. Com a promulgação da Medida Provisória 2200-2/01, o que se percebe é que essa discussão quanto à autenticidade e integridade dos documentos digitais com assinatura digital foi superada. Essa lei, que instituiu em seu artigo primeiro a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), tem como finalidade garantir a autenticidade, a integridade e a validade jurídica de documento em forma eletrônica, bem como a realização de transações eletrônicas seguras.

Os documentos assinados dessa forma têm, portanto, valor probante *erga omnes*. Essa Medida Provisória dá uma solução jurídica para os arquivos eletrônicos com assinatura digital. Mas, o que fazer com a maioria dos arquivos, que não possuem assinatura digital?

Caso haja qualquer dúvida quanto à autenticidade, poderá ainda ser feita uma perícia técnica, da mesma forma como é feita com as representações mecânicas utilizadas como prova. É nesse contexto que a tecnologia em muito contribui para o direito à medida

que fornece mecanismos para atestar identidade, autoria, integridade e acessibilidade. Caso o documento não tenha certificação digital, é possível atestar sua autenticidade e integridade por meio de perícia técnica.

A Forense Digital, subárea da Ciência Forense, apresenta um conjunto de técnicas utilizadas para coletar, reunir, identificar, examinar, correlacionar, analisar e documentar evidências digitais processadas, armazenadas ou transmitidas por computadores. É amplamente utilizada no Direito Penal, como instrumento para agregar valor probatório às evidências detectadas.

Face ao grau de complexidade dos sistemas e softwares a serem analisados, torna-se necessário que os profissionais da área sejam os responsáveis pelas investigações forenses nesse campo. Além disso, há que utilizar as ferramentas adequadas, evitando assim que qualquer procedimento comprometa as evidências a serem examinadas. Na análise de uma máquina, são utilizadas ferramentas específicas com o objetivo de não modificar o sistema em investigação.

Portanto, tanto os documentos eletrônicos assinados digitalmente, como aqueles que não possuem assinatura digital podem e devem ser utilizados como evidência legal, sendo que o seu grau de validade jurídica estará associado à forma como tiverem sido gerados, armazenados e preservados. Ou seja, vale reforçar que mesmo os documentos não assinados digitalmente têm valor probatório e podem ser objeto de perícia, vide os arquivos obtidos nos casos de apreensão de computadores, seja para um fim qualquer (penal, civil, tributário,...). Ainda, mesmo que as informações digitais não sejam provas em si, podem ser utilizadas ao menos como um norte para chegar a elucidação dos crimes analisados.

Tanto o Código de Processo Civil como o Código de Processo Penal estabelecem que quando a prova do fato depender de conhecimento técnico ou científico, o juiz será assistido por perito, que deverá entregar o laudo no prazo fixado pelo juiz. O juiz aplicará as regras de experiência comum subministradas pela observação do que ordinariamente acontece e ainda as regras da experiência técnica, ressalvado, quanto a esta, o exame pericial. O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte.

A perícia em informática é responsável, portanto, por produzir laudos periciais com o objetivo de determinar a dinâmica, a materialidade e a autoria dos atos ilícitos. Assim, tem como principal finalidade identificar, processar e transformar evidências digitais em

provas materiais de crimes utilizando métodos técnico-científicos, com o objetivo precípuo de conferir-lhes validade probatória em juízo.

Diante da ausência de normas específicas na legislação brasileira para a investigação em âmbito computacional, as normas gerais para todo tipo de perícia criminal definidas no Código de Processo Penal devem ser adotadas, com o fito de garantir que os vestígios encontrados possam ter algum valor probatório.

O processo de perícia em informática começa, por conseguinte, a partir de um mandado judicial. Daí é feita a coleta no local do crime, a apreensão, a preservação do material coletado, a duplicação do material coletado, a análise que é feita nas cópias e, por fim, a documentação da análise que é colocada em um Laudo Pericial.

No caso de crimes cibernéticos, as evidências podem estar presentes em mensagens de correio eletrônico e bate-papo, imagens de pornografia infantil, dados cifrados, registros de impressão, engenharia reversa de programas, conversão de banco de dados, registros de conexão à Internet e fragmentos de arquivos. A perícia pode ser realizada em mídias digitais, máquinas caça-níqueis, aparelhos celulares, ou mesmo na Internet.

Em um julgamento, garantir a continuidade das evidências é essencial para a formação da convicção do juiz ou do júri. Qualquer dúvida quanto a essa continuidade, pode levar à invalidade da prova. Assim, para garantir que os resultados da investigação forense tenham valor probatório, torna-se essencial seguir determinados protocolos que assegurem que as evidências sejam coletadas, preservadas e analisadas de forma minuciosa e livre de contaminações. Com o objetivo de garantir a autenticidade e a integridade das evidências digitais analisadas, os procedimentos adotados no processo de investigação forense devem, portanto, atender aos princípios e boas práticas dos profissionais da área.

O processo de investigação forense deve garantir a autenticidade e a integridade das evidências coletadas e dos resultados produzidos. Isso implica dizer que deve garantir que as informações obtidas estejam presentes nas evidências analisadas e não tenham sido alteradas ou contaminadas pelo processo de investigação. Devido ao alto grau de volatilidade das evidências digitais, isso é particularmente difícil. Portanto, torna-se essencial que se siga um método consoante a tecnologia envolvida.

Antes de iniciar a inspeção, torna-se necessário afastar qualquer pessoa do equipamento analisado, com o objetivo de impedir que qualquer prova seja plantada ou que as evidências sejam danificadas. Essa atividade é definida como ***Quarentena***. Além disso, é

essencial uma completa inspeção visual com a devida utilização de fotografias e anotação de tudo que for importante a fim de garantir que nenhuma informação seja perdida e todos os riscos sejam devidamente considerados.

Quanto melhor for definido o processo de análise forense, maiores serão as chances de sucesso. Assim, torna-se importante detalhar os procedimentos utilizados, bem como o uso de determinadas ferramentas e técnicas. Além disso, os princípios e boas práticas supracitados devem guiar o trabalho a ser executado para garantir o sucesso da investigação a ser realizada.

Dentre as etapas que compõe o processo de investigação forense, a mais importante é a responsável pela ***coleta das informações do sistema suspeito.*** Essa etapa, se conduzida de forma inadequada, pode comprometer toda a investigação forense. Os dois grandes perigos, que devem ser evitados a todo custo, são a perda e a alteração do material de análise. Assim, toda informação deve ser tratada como se fosse utilizada para fins judiciais. Além disso, respeitando a ordem de volatilidade, deve ser coletada a maior quantidade possível de evidências. Cada item coletado deve ser autenticado, identificado, catalogado e preservado. Por fim, devem ser produzidas cópias exatas e autenticadas das informações digitais coletadas.

Os modelos sugeridos para análise e identificação das evidências digitais são exemplos de como o perito pode estudar e buscar as evidências no material coletado para análise, bem como direcionar o trabalho de análise. O modelo que relaciona papéis desempenhados por um determinado dispositivo digital é importante para avaliar o potencial de cada dispositivo como prova em uma determinada situação. O modelo dos sete elementos permite identificar as fragilidades do sistema e suas vulnerabilidades. Por fim, o terceiro modelo apresentado, permite detectar o grau de responsabilidade de cada usuário na atividade realizada. Esses modelos são usados na fase de análise das evidências digitais

A ordem de volatilidade das evidências digitais determina que seu tempo de vida varie de acordo com o local de armazenamento. Quanto maior a volatidade de uma determinada informação, mais difícil se torna sua extração e menos tempo há para capturá-la. Informações voláteis tais como o conteúdo da memória principal e dos dispositivos de armazenagem secundária, bem como, o estado do sistema operacional, podem conter informações valiosas a respeito dos atos ilícitos cometidos e podem determinar seus responsáveis.

Os ***dispositivos de armazenagem secundária*** representam a maior fonte de informação para a análise forense. Além de ser uma memória não volátil, sua capacidade de armazenamento é enorme. O ***sistema de arquivos*** é a fonte de informação básica para a análise forense. É a parte do sistema operacional responsável por organizar as informações do disco na forma de arquivos. Cada sistema operacional possui a sua forma de organizar os arquivos. A quantidade e a qualidade das pistas deixadas nas estruturas de dados do sistema de arquivos irão determinar o número de informações que podem ser recuperadas.

O guia de boas práticas para evidências eletrônicas requer que o exame dos dispositivos digitais seja feito de forma a minimizar a possibilidade de contaminação digital. Ainda, a autenticidade e a integridade das informações digitais coletadas podem ser estabelecidas por meio de assinaturas criptográficas, como o MD5 e o SHA. É possível determinar a autenticidade de uma informação digital coletada por meio da simples comparação entre o seu hash criptográfico com a assinatura criptográfica da informação original.

O laudo pericial representa a materialização da prova pericial. Portanto todo laudo pericial deve ser feito com qualidade, pois contribui para a formação da convicção do juiz. Para tanto, deve ser claro, objetivo e conciso, abstendo-se de julgamentos com bases pessoais do perito e deve conter a fundamentação e a conclusão as quais o perito chegou. Deve primar pelo rigor tecnológico, atendo-se, portanto, a sua área de conhecimento. Além disso, deve apresentar os documentos, evidências e meios necessários à formação da convicção do juiz. Caso não seja claro, o CPC permite que seja realizada segunda perícia, quando possíveis omissões ou inexatidão poderão ser saneadas.

Quando se pensa em provas, pensa-se na relação entre os vestígios. Essa relação deve ser demonstrada de forma exata no laudo pericial, que deve apontar a extensão e a causa do fato, indicando se houve negligência, imprudência, imperícia ou dolo, por exemplo.

Diante do exposto, fica claro que o respeito às normas técnicas e científicas para a realização de uma perícia digital garante o valor probatório dos arquivos digitais obtidos, sendo possível, portanto, garantir a autenticidade e a integridade dos mesmos. O calcanhar de Aquiles da proposta apresentada refere-se à fase anterior à quarentena, quando um perito mal-intencionado ou uma série de gatilhos poderiam alterar as propriedades ou implantar arquivos nos dispositivos digitais analisados.

Ocorre que, se por um lado, apesar de ser possível alterar os dados presentes nos dispositivos, por outro, pelo princípio de Locard, é impossível apagar todos os rastros dessa atividade. O princípio fundamental da Ciência Forense é conhecido como ***Princípio de Intercâmbio*** ou ***Princípio de Locard*** que estabelece que quando um indivíduo entra em contato com um objeto ou outro indivíduo, sempre deixa vestígio desse contato. Não há como eliminar todos os rastros.

Nesse cenário, caso o juiz considere o laudo impreciso, pode solicitar segunda perícia, o que permitirá, por meio da análise dos arquivos de log, identificar o histórico de modificações ocorrido nas evidências detectadas. Mais uma vez, percebe-se que o valor probatório dos arquivos digitais foi mantido.

Diante da crescente expansão e disseminação dos recursos tecnológicos, torna-se imperativa, portanto, a aceitação do uso dos arquivos digitais nos processos judiciais. Assim, os arquivos digitais gerados pelos serviços de home banking, as informações comprobatórias de desvio de fluxo de caixa extraídas de computadores confiscados pelos fiscais da Receita Federal, o material pornográfico infantil rastreado e fornecido pelos provedores de acesso são exemplos evidentes de sua força probatória e, devem, portanto, ser usados como prova, auxiliando assim na formação da convicção do juiz.

REFERÊNCIAS BIBLIOGRÁFICAS

CALAZANS R., Carlos Henrique; CALAZANS, Sandra Maria Pereira Benone. **Ciência Forense: das origens à ciência forense computacional**. XV SEMINÁRIO REGIONAL DE INFORMÁTICA, 2005. Santo Ângelo, RS. Anais do 15º Seminário Regional de Informática. Santo Ângelo. RS : Universidade Regional Integrada do Alto Uruguai e das Missões, 2005.

DEL CAMPO, Eduardo Roberto Alcântara. **Exame e levantamento técnico pericial de locais de interesse à justiça criminal: abordagem descritiva e crítica**. – São Paulo: E.R.A. Del-campo, 2008.

DINIZ, Davi Monteiro. **Documentos eletrônicos, assinaturas digitais: da qualificação jurídica dos arquivos digitais como documentos**. São Paulo: LTr, 1999.

FARMER, Dan; VENAMA, Wietse. **Perícia forense computacional:** teoria e prática aplicada. São Paulo: Pearson Prentice-Hall, 2007.

GEUS et alli. Forense **Computacional: aspectos legais e padronização**. Disponível em: <http://www.las.ic.unicamp.br/paulo/papers/2001-WSeg-flavio.oliveira-marcelo.reisforense.pdf >. Acessado em: 15 de Maio de 2011.

GICO JUNIOR, Ivo Teixeira. – **A assinatura eletrônica**. IOB-Repertorio de Jurisprudencia: tributária, constitucional. 2000a. Biblioteca(s): DCV. Assunto: Documento Eletrônico. Idioma: POR. – Disponível em: http://works.bepress.com/ivo_teixeira_gico_junior/9.

GICO JUNIOR, Ivo Teixeira. -- **O arquivo eletrônico como meio de prova**. IOB-Repertorio de Jurisprudência: civil, processual, penal e comercial. São Paulo. n.15. p.329-325. ago. 2000b.

GICO JUNIOR, Ivo Teixeira. -- **O conceito de documento eletrônico**. IOB-Repertorio de Jurisprudência: civil, processual, penal e comercial. São Paulo. n.14. p.306-302. jul. 2000c.

Good Practices guide for computer based evidence. Association of Chief Police Officers of England, Wales and Northern Ireland, Junho de 1999. ACPO Crime Commitee. Disponível em: <http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf>

LOPES, Marilu; GABRIEL, M. M.; BARETA, G. M. S. **Cadeia de custódia: uma abordagem preliminar**. Sistema eletrônico de Revistas da UFPR. Disponível em: < http://ojs.c3sl.ufpr.br/ojs2/index.php/academica/article/viewfile/9022/6315 >. Acessado em 28 de Junho de 2011.

MARTINEZ, Antonio Javier García. **La formacion de um IRT**. Disponível em: < http://www.e-evidence.info/international.html >. Acessado em 15 de Maio de 2011.

MIRABETE, Júlio Fabbrini. **Processo penal**. 18ª Edição, Revista e atualizada. São Paulo: Editora Atlas S.A., 2006.

MITTERMAIER, C. J. A. **Tratado da prova em matéria criminal ou exposição comparada**. Trad. Herbert Wüntzel Heirich. Campinas: Bookseller, 1997.

MARSHALL, Angus M. **Digital forensics in criminal investigation**. Editora Wiley-BlackWell, 2008.

NOBREGA, João. **Captura de computadores de Bin Laden pode ser filão de informação sobre a Al-Qaeda.** IDG NOW. Computer World. Seção Segurança. Disponível em: <

http://idgnow.uol.com.br/seguranca/2011/05/04/captura-de-computadores-de-bin-laden-pode-ser-filao-de-informacao-sobre-a-al-qaeda/>. Lido em 04/05/2011.

PINHEIRO, Patrícia Peck. -- **A questão da prova legal na sociedade digital**. Revista do Tribunal Regional Federal da 3ª Região. São Paulo. n.78. p.9-30. jul./ago. 2006. Biblioteca(s): DPC.

PIRES, Paulo S. da Motta. **Forense computacional: uma proposta de ensino.** Disponível em: <http://www.leca.ufrn.br/~pmotta/ensino-forense.pdf>. Acessado em: 15 de Maio de 2011.

REIS, Marcelo Abdalla dos; GEUS, Paulo Lício de. **Análise forense de intrusões em sistemas computacionais: técnicas, procedimentos e ferramentas.** Disponível em < http://www.truzzi.com.br/blog/wp-content/uploads/2010/07/Monografia_AnaliseForense.pdf >. Acessado em 15 de Maio de 2011.

REIS, Marcelo Abdalla dos; GEUS, Paulo Lício de. **Forense computacional: procedimentos e padrões**. Disponível em <http://www.las.ic.unicamp.br/paulo/papers/2001-SSI-marcelo.reis-forense.padroes.pdf>. Acessado em 15 de Maio de 2011.

URDANETA, Iraset Páez. **Gestión de la inteligencia, aprendizaje tecnológico y modernización del trabajo informacional - retos y oportunidades**. Caracas/Venezuela, Instituto de Estudios del Conocimiento de La Universidade Simon Bolivar/Consejo Nacional de Investigaciones Cientificas Y Tecnologicas, 1992, 99-112.

PROSISE, Chris; MANDIA, Kevi. **Incident Response & Computer Forensics**. New York: Ed. McGraw-Hill, 2003.

ANEXO I – FERRAMENTAS DISPONÍVEIS

Diante da quantidade de arquiteturas e sistemas operacionais disponíveis no mercado, o investigador deve ter um conjunto de ferramentas que o ampare no processo de coletar, documentar, preservar e processar as informações oriundas do sistema suspeito.

A primeira ferramenta e a mais importante é uma ***estação forense***, local onde a análise das informações coletadas será feita. Essa estação deverá ter os dispositivos de hardware e software necessários a coleta, documentação, preservação e análise das informações oriundas do sistema suspeito. Deve ser uma máquina portátil, com alta capacidade de processamento e armazenamento de dados, com interface de rede e que permita a conexão com vários tipos de periféricos.

Quanto ao ***sistema operacional***, ainda que esteja relacionada à preferência do investigador, muitas vezes é fundamental adotar a mesma plataforma encontrada no sistema suspeito. Além disso, ter os programas de instalação dos principais sistemas operacionais, nas mais variadas versões, possibilitará recriar o ambiente do sistema investigado. Outra possibilidade não menos interessante é adotar uma máquina virtual como o VMShare que permita instalar diferentes sistemas operacionais e efetuar a escolha de acordo com a necessidade.

Para efetuar a ***coleta e a análise de informações*** é necessário ter um conjunto de utilitários confiáveis que possam conduzir a investigação. Esses utilitários devem ser compilados estaticamente ou devem estar em um CDROM que contenha cópias seguras das bibliotecas dinâmicas visando evitar problemas com programas alterados na máquina suspeita. Uma solução possível é adotar o CDROM ISO 9660 que contém um grande número de utilitários (binários e scripts) que possibilitam acessar qualquer plataforma.

Dentre outras ferramentas úteis, pode-se citar versão de sistema operacional que caiba em mídia removível que não execute qualquer operação na área de armazenagem, além de outros itens auxiliares destinados à desmontagem das máquinas; identificação, transporte e armazenagem de materiais coletados; e documentação das atividades. Como exemplo, pode-

se citar máquina fotográfica, mídia removível, disco rígido, cabos e conectores de rede, etiquetas e formulários, parafusos, alicates, dentre outros.

O investigador deve estar familiarizado com as ferramentas disponíveis e deve ter noção do impacto que seu uso pode provocar no sistema suspeito. Por isso, antes de começar a usá-las, deve praticar e testar para ter conhecimento e certeza quanto ao funcionamento das mesmas.

No mercado, há ferramentas disponíveis para preservação e para coleta de evidências. Uma das ferramentas mais importantes para preservação da situação atual do sistema suspeito é a ***Tribble***[104]. Desenvolvida por Joe Grand, essa ferramenta é um cartão de expansão de hardware que pode capturar de forma confiável a memória volátil de um sistema vivo de armazenamento removível. Esse dispositivo de hardware acessa diretamente a memória e não precisa de software para ser carregado, o que poderia sobrescrever uma possível evidência.

Outra ferramenta de suma importância para o processo de análise das informações do sistema de arquivos é o hash criptográfico. O propósito do hash de um arquivo é estabelecer uma assinatura desse arquivo em seu estado confiável, sendo utilizada para checagem de integridade. Esse processo de criação de bases de assinaturas criptográficas e checagem de integridade pode ser totalmente automatizado com a utilização de ferramentas como o ***Tripwire***[105].

Dentre as ferramentas que podem ser utilizadas para procurar evidências digitais, pode-se-ia citar o ***TCT-utils***, o ***Sleuth Kit,*** o ***Autopsy Forensic Browser*** e o ***Mac-robber***. Substituído pelo seu sucessor oficial Sleuth Kit (TSK[106]), o ***Coronel's Toolkit (TCT)***[107] foi uma das primeiras e mais importantes ferramentas desenvolvidas para a análise forense computacional. Desenvolvido por Dan Farmer e Wietse Venema em Agosto de 1999, é um conjunto de ferramentas de linhas de comando de código aberto e gratuito que permite investigar um sistema UNIX comprometido. Inicialmente não foi desenvolvido para apresentar evidências úteis em um processo criminal, e sim para ajudar a identificar o que aconteceu em um sistema invadido. Seu desenvolvimento parou há alguns anos.

---

[104] Tribble pode ser encontrada na URL http://www.grandideastudio.com/portfolio/tribble/
[105] Para obter mais informações, acesse o site HTTP://www.tripwire.com .
[106] TSK pode ser encontrado na URL http://www.sleuthkit.org/index.php
[107] TCT pode ser encontrado na URL HTTP://www.porcupine.org/forensics/tct.html

Sucessor do TCT, o ***Sleuth Kit*** é uma coleção de ferramentas de linha de comando baseada em UNIX que permite que um investigador leia os arquivos e conteúdos deletados no NTFS, FAT, FFS e imagens do sistema de arquivo EXT3FS e EXT2FS. Essa ferramenta também permite que o investigador realize pesquisas de banco de dados hash e classifique arquivos baseados nessa estrutura. O TSK pode ser integrado em um sistema forense automatizado de diversas formas e pode ser executado em Linux, OS X, FreeBSD, OpenBSD, and Solaris e pode analisar FAT, NTFS, UFS, EXT2FS, e EXT3FS. O navegador Autopsy pode ser usado com TSK para automatizar muitas dessas funções. Ambos são sistemas abertos e podem ser executados em plataformas UNIX.

Desenvolvida por Brian Carrier, a ferramenta ***Autopsy Forensic Browser*** torna a investigação do sistema muito mais fácil e rápida. Com interface gráfica baseada em HTML, permite que um investigador analise uma imagem de sistema de arquivos a partir de um gerenciador de arquivos próprio, visualize espaços e estruturas de dados não alocados, faça cronogramas de atividade dos arquivos e realize buscas de palavras-chave.

O ***Mac-Robber*** é uma ferramenta de investigação digital que coleta dados a partir de arquivos alocados em um sistema de arquivos. Coleta os horários de criação, alteração e acesso dos arquivos e pode ser usado em conjunto com o Sleuth kit para gerar o cronograma de atividades dos arquivos.

Fundada em 1996, a empresa NTI[108] é uma das empresas mais importantes no campo da investigação forense. Oferece consultoria, treinamentos e ferramentas com diferentes finalidades, incluindo resposta a incidentes, extração e proteção de evidências, limpeza de discos e produção de imagens. Dentre as inúmeras ferramentas desenvolvidas, poder-se-ia citar:

a) AnaDisk – Ferramenta de análise de disquetes usado para identificar anomalias em padrões de armazenamento;

b) CopyQM – Utilitário de duplicação de disquete usado para produzir disquetes em massa para uso em processamento de dados e na criação de disquetes de auditoria de segurança .

c) CrcMD5 - Cria uma assinatura hash para um ou mais arquivos presentes em um dispositivo de armazenamento.

[108]Maiores informações sobre a empresa NIT podem ser encontradas no site http://www.forensics-intl.com/index.html

d) DiskScrub - Utilitário de segurança que é usado para destruir dados de forma segura em uma unidade de disco rígido do computador.

e) DiskSig Pro – Utilitário que valida a integridade de um sistema original e expande as capacidades do utilitário DiskSig.

f) FileList Pro – Utilitário de catalogação de discos para uso em todos os sistemas operacionais da Microsoft. Esta ferramenta também pode ser usada na avaliação dos cronogramas de atividade.

g) File Convert Pro - Uma ferramenta de conversão de dados que é usada para descompactar os arquivos criados pelo utilitário FileList Pro.

h) FileCNVT - Utilitário usado para descompactar arquivos criados com o programa FileList original.

i) Filter_G - Usado para identificar padrões da gramática da língua Inglês e estrutura da frase em fontes de dados usuais.

j) Filter_I - Usaada para documentar resultados das fontes de dados usuais.

k) Filter_N – Filtro forense filtro na identificação de formatos de número relevante. Esta ferramenta é útil em investigações relacionadas com o roubo de identidades.

l) FNames – Banco de dados forense patenteado que identifica automaticamente nomes de indivíduos europeus, em inglês, e árabes. Esta ferramenta é muito importante em missões de espionagem e, em casos de roubo de identidade.

m)GetFree - Instrumento de coleta de dados forenses utilizado em revisões de segurança e investigações relacionadas com a captura de dados e fragmentos de arquivos associados a arquivos excluídos anteriormente.

n) GetGIF - Filtro de dados forenses que identifica automaticamente e reconstrói com precisão arquivos de formato GIF a partir de fontes de dados de computador. Esta ferramenta é doada gratuitamente para especialistas em crimes de informática com o objetivo de auxiliar nas investigações que envolvem a distribuição ilegal de pornografia infantil

o) GetNames - Ferramenta que identifica automaticamente nomes próprios em Inglês armazenados em dispositivos de informática. Esta ferramenta é doada gratuitamente a especialistas em crimes de informática para auxiliar nas investigações de fraude.

p) GetHTML - Ferramenta utilizada para identificar e extrair documentos HTML armazenados em dados usuais e / ou dispositivos de informática. Esta ferramenta é doada

gratuitamente a especialistas em crimes de informática para auxiliar nas investigações relacionadas a Internet.

q) Graphics File Extractor - Filtro de dados forenses que identifica automaticamente e reconstrói com precisão arquivos nos formatos BMP, GIF JPG a partir de fontes de dados do computador. Esta ferramenta é especialmente útil em casos de roubo de identidade e casos que envolvem pornografia.

r) HexSearch - Ferramenta de pesquisa forense de dados binários usada para identificar arquivos gráficos e/ou palavras e frases em língua estrangeira armazenadas no computador.

s) NTA Stealth – Ferramenta utilizada para determinar quando um computador foi usado para acessar sites de pornografia na Internet.

t) NTI Secure ToolKit – Ferramenta de criptografia de arquivos.

u) M-Sweep XP - Utilitário de segurança que elimina de forma segura dados de folgas de arquivo, espaço não alocados, arquivos apagados, páginas de swap do Windows e arquivos de paginação em DOS, Windows, Windows 95, Windows 98, Windows NT, Windows 2000 e sistemas de computador com Windows XP.

v) SafeBack 3.0 - Usado para criar imagem de espelho (fluxo de bits) de arquivos de backup de discos rígidos ou fazer uma cópia de espelho-imagem de um disco rígido inteiro ou deuma partição. O processo é análogo ao da fotografia e da criação de um negativo fotográfico.

w) TextSearch Plus - Utilitário de pesquisa de texto usado em revisões de segurança e investigações criminais em sistemas baseados em DOS, Windows, Windows 95 e Windows 98 para localizar palavras-chave específicas, cadeias de texto e arquivos gráficos.

x) TextSearch NT - Utilitário de pesquisa de texto usado em revisões de segurança e investigações criminais em sistemas baseados em FAT 32, Windows NT, Windows 2000 and Windows XP para localizar palavras-chave específicas, cadeias de texto e arquivos gráficos

Outra empresa de destaque na área de investigação forense é a Guidance Software. Seus serviços incluem resposta a incidentes, consultoria e ferramentas com diferentes finalidades. Uma das ferramentas é o ***EnCase ® Portable*** que é um dispositivo de bolso USB destinado a coleta de evidências digitais e triagem. Projetado para permitir que qualquer pessoa pesquise, colete e analise os dados, sem comprometer a integridade forense dos dados adquiridos.

Solução de investigação padrão da indústria de computadore, o ***EnCase*** ® ***Forensic***, é destinado aos profissionais forenses que necessitam realizar um coleta de dados com um processo bem definido. Permite adquirir dados de uma ampla variedade de dispositivos, bem como gerar relatórios das evidências detectadas, garantindo , a integridade das provas. O EnCase não opera na mídia original ou nos discos espelhados. Em verdade, monta os arquivos de evidências como discos virtuais protegidos contra escritas. Assim, permite que o investigador visualize, ordene e analise os dados, por meio de uma interface gráfica.