Um olhar sobre a perícia forense computacional, a aplicação da coleta, a preservação de provas em ambientes digitais e a formação da cadeia de custódia, segundo a ISO 27.037,[1] a Lei nº 13.964[2] e o PL nº 4939/2020, impulsionado pela anulação de provas obtidas em sistemas da Odebrecht em todas as esferas e para todas as ações do Supremo Tribunal Federal (STF)

Ricardo Andrian Capozzi

Bacharel em Direito e Tecnologia da Informação e Ciência da Computação pela Faculdade de Informática e Administração de São Paulo (1995). Atuou 25 anos como consultor para Banco Citibank S.A. nas áreas de processos de segurança e sistemas de plataformas eletrônicas e *internet banking*. Professor e pesquisador da Faculdade Drummond (Instituto de Pós-Graduação e Graduação – IPOG; Instituto Mauá de Tecnologia – IIMT); da Faculdade de Tecnologia (FATEC) e da Universidade Presbiteriana Mackenzie para as cadeiras de Segurança da Informação, Auditoria e Compliance, Redes de Dados, Sistemas Operacionais e Resposta a Incidentes de Segurança da Informação. Palestrante e consultor assistente judicial *ad hoc*. Perito do juízo nomeado para o TRT, TFT e TJ de São Paulo.

Resumo: A cadeia de custódia[3] contribui com a validação de uma prova pericial obtida, examinada e apresentada em um trabalho que se consubstancia em um relatório denominado laudo pericial. A formatação de uma prova é essencial para que se estabeleça o correto processo legal, e para que este possa ser, a qualquer tempo, replicado ou reproduzido segundo algum método científico que seja

[1] Disponível em: https://www.iso.org/standard/44381.html. Acesso em: 5 mar. 2018.

[2] A Lei nº 13.964, de 24 de dezembro de 2019, conhecida como Pacote Anticrime, alterou 17 leis, dentre as quais o Código Penal, o Código de Processo Penal e a Lei de Execuções Penais – com profundos reflexos no sistema de justiça criminal brasileiro.

[3] "Art. 158-A do CPP. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. (Incluído pela Lei nº 13.964, de 2019)."

aceito pela comunidade acadêmica e tenha valor jurídico. A responsabilidade pela manutenção da lisura e idoneidade processual é compartilhada por todos os atores envolvidos na lide, com atenção ao perito judicial, pois é sobre seus ombros que recai a responsabilidade pela obtenção da prova e pela manutenção da cadeia de custódia. A necessidade de procedimentos operacionais padronizados é fundamental para que, diante dos questionamentos apresentados pelo juízo e patronos, as provas periciais continuem robustas e confiáveis, baseando o livre convencimento do magistrado em sua sentença. Por fim, o Projeto de Lei nº 4.939/2020[4] trata das diretrizes do Direito da Tecnologia da Informação e das normas de obtenção e de admissibilidade de provas digitais na investigação e no processo, além de outras providências. Até o momento da escrita deste artigo, porém, não foi votado ou incorporado ao ordenamento jurídico brasileiro. Em 6 de setembro de 2023, durante a "Operação Spoofing", o ministro Dias Toffoli (STF) deferiu a medida que torna nulas todas e quaisquer provas obtidas dos sistemas Drousys e My Web Day B, utilizadas a partir do acordo de leniência celebrado pela Odebrecht, no âmbito da "Operação Lava Jato". A decisão atacada no mérito atende à Reclamação nº 4.3007 e torna imprestáveis, em definitivo, com efeitos *erga omnes*, as provas e os demais elementos obtidos a partir desse acordo, em qualquer âmbito ou grau de jurisdição com base em elementos de prova contaminados. A metodologia utilizada neste trabalho, amplamente aceita e difundida, é a da coleta e do estudo de referencial teórico, com análise de normativa da ABNT. Visa, por fim, dar sustentação jurídica à necessidade da coleta de provas em dispositivos eletrônicos e colabora com os *experts* na área da forense computacional ao mostrar que a prova digital tem particularidades incomparáveis com outros meios de produção de prova, e que alguns elementos que a fazem valer em um tribunal são a derivação e a formatação de sua cadeia de custódia.

Palavras-chave: Cadeia de custódia. Perícia grafotécnica. Direito. Provas.

1 Introdução

A produção de prova tem sua base no direito constitucional de ação e de defesa, inserida pelo artigo 5º, inciso XXXV, da Constituição Federal de 1988. Segundo Silva (2009, p. 431), além do direito de provocar a atividade jurisdicional, como direito público subjetivo de agir, também se tutela contra quem propõe a ação, assegurando o contraditório e a ampla defesa. A prova garante o direito à ampla defesa e assegura o direito ao devido processo legal. A segurança constitucional, mesclada ao direito de acesso à Justiça, ao contraditório e à plenitude de defesa fecham o ciclo das garantias individuais da pessoa humana.

A prova pericial é a única fonte objetiva das provas. Dentre as produzidas na fase de persecução penal, é a que mais baliza a decisão dos juristas e do júri, por seu poder de convencimento, amparado por características como imparcialidade e embasamento científico. Um procedimento dessa natureza, por foça de lei, como

[4] O projeto estabelece regras para a obtenção e admissibilidade de provas digitais em processos criminais. Isso inclui a possibilidade de infiltração de agentes de investigação em redes de dados.

estabelece o Código de Processo Civil em seu artigo 170, deve ter a qualidade de ser reproduzido e replicado, quando houver necessidade de corroboração do fato em laboratório: "(...) 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." Tal fato se deve à exigência da lei pela guarda de amostras dos materiais analisados, pois fiducia ao investigado a possibilidade de contestação e a defesa *a posteriori*.

De acordo com Espíndula (2009), existe a prática de alguns patronos de questionar o manuseio de evidências, para, quando necessário, favorecer uma das partes interessadas; e de colocar em xeque que uma das etapas da formatação da cadeia de custódia foi falha e, portanto, que todas as evidências colhidas na cena de um crime estão viciadas ou contaminadas. Assim, o procedimento costuma ser enormemente explorado como argumento de defesa.

Entretanto, por mais que os avanços tecnológicos e científicos tenham contribuído com a disciplina forense, não representam uma garantia certa de que essas evidências serão aceitas como prova pericial pela Justiça (Júnior, 2012).

Assim, para avalizar a validade dos exames periciais e dos métodos aplicados na busca, coleta e classificação das evidências, os doutos peritos devem respeitar a cadeia de custódia, que trata da documentação que o laboratório possui com a intenção de rastrear todas as operações realizadas com cada vestígio deixados pelo crime – corpo de delito, desde a coleta no local do crime até a completa destruição (Chasin, 2008). Outra descrição que bem serve para o termo analisado é dada por Nascimento (2013):

> A Cadeia de Custódia é um processo de documentar a história cronológica da evidência, esse processo visa a garantir o rastreamento das evidências utilizadas em processos judiciais, registrar quem teve acesso ou realizou o manuseio desta evidência. Se faz necessária em todas as atividades profissionais onde possa ocorrer situações que resultem em processos judiciais.

O termo pode também ser colocado ao se referir como garantidos de identidade e integridade de uma amostra pericial, desde o instante da coleta até a entrega dos resultados. No Brasil, onde não há uma normativa geral sobre a cadeia de custódia, cerne da preservação das informações coletadas, ela possibilita documentar a cronologia das evidências, identificá-las por seu manuseio etc. Procedimentos técnicos como lacres e restrição de acesso aos profissionais responsáveis pela custódia, em seu manuseio, minimizam a possibilidade da manipulação indevida e tornam as evidências mais confiáveis, que ganham valor probatório (Brasil, 2012).

O artigo 6º do Código de Processo Civil diz que a cadeia de custódia[5] se inicia logo após o conhecimento do fato delituoso e que a autoridade policial deve garantir a conservação da cena do crime, evitando manipular indícios do local do fato.

> Art. 6º - Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
> I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias.

Ainda por Espíndula (2009), os elementos que darão origem às provas periciais ou documentais solicitam cuidados a fim de resguardar a confiabilidade e a idoneidade no decorrer de todo o processo de investigação e de trâmite judicial. A documentação fundamental relacionada a uma cadeia de custódia deve conter, necessariamente, os seguintes itens:

> a. Quem coletou e manuseou a amostra.
> b. Quais amostras foram manuseadas.
> c. Quando tais amostras foram manuseadas.
> d. Autores que manusearam a amostra.
> e. Local de permanência da amostra.

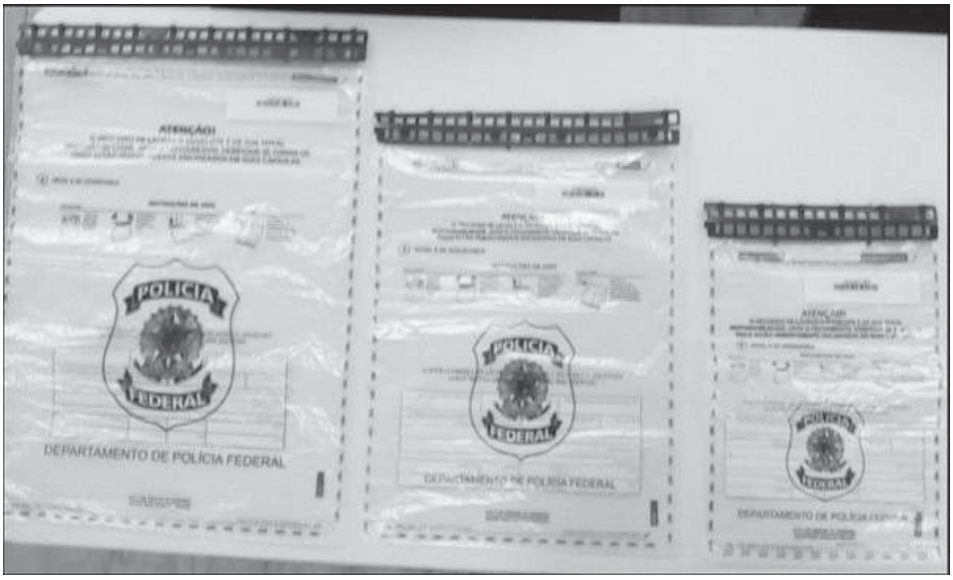
Já a Associação Brasileira De Normas Técnicas, dada pela NBR 27.037, com as diretrizes para identificação, coleta, aquisição e preservação de evidências digital, em seu subitem 6.1, convenciona que o registro de cadeia de custódia contenha no mínimo as seguintes informações:

> a. Identificador único da evidência.
> b. Quem acessou a evidência e o tempo e local em que ocorreu.
> c. Quem checou a evidência interna e externamente nas instalações de preservação da evidência e quando ocorreu.
> d. Motivo de a evidência ter sido verificada (qual caso e propósito) e a autoridade relevante, se aplicável.
> e. Quaisquer alterações inevitáveis da potencial evidência digital, assim como o nome do indivíduo responsável para tanto e a justificativa para a introdução da alteração.

[5] Uma tradução livre poderia ser, no contexto legal, o procedimento que se refere-se à documentação cronológica ou histórica que registra a sequência de custódia, controle, transferência, análise e disposição de evidências físicas ou eletrônicas

Independentemente do estado da prova, se objeto físico ou digital, em qualquer meio, ela deve ser acondicionada em dispositivos apropriados e específicos para o uso, de forma a ser inviolável e permitir identificar e garantir quem e por onde foi manuseada.

Figura 1 – Exemplos de sacos para custódia de evidências.
Início da criação da cadeia de custódia



Fonte: Arquivo pessoal.

Figura 2 - Saco de evidências. Detalhes para os campos de identificação

Fonte: Arquivo pessoal.

Figura 3 - Forma de armazenamento incorreta para prova judicial

Fonte: Backupday (2018).

No que diz respeito ao perito, é imprescindível que este conheça o Código de Processo Penal, "Capítulo II - Do Exame do Corpo de Delito e das Perícias em Geral". Os seguintes artigos devem ser observados quando da obtenção de uma evidência:

> Art. 170. Nas pericias 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, alem de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado.

Assim, ao lermos o artigo 170 do Código de Processo Penal, subentendemos a necessidade de o perito fazer cópias com assinaturas digitais (*hashs*), para a manutenção da integridade e as análises futuras de uma prova digital.

Ainda segundo Galvão (2011), apesar da falta de padronização, a atividade pericial é legalmente reconhecida no estado de São Paulo, conforme Decreto nº 48.009, de 11 de agosto de 2003. Seu artigo 12, que fala que o Núcleo de Perícias de Informática, tem por atribuição realizar perícias visando à elaboração de laudos periciais de locais e peças envolvendo aparelhos computadorizados, a exemplo de sistemas de *software*, equipamentos de *hardware* e periféricos, relacionados com a prática de infrações penais na área de informática ou redes de dados.

2 Forense computacional

A arte forense computacional[6] abrange questões relacionadas aos crimes praticados pela *internet* ou tendo o computador como meio ou fim de um delito, crimes esses conhecidos como próprios ou impróprios e chamados pela mídia de cibercrimes (Farmer, 2007). A referida arte concentra-se em estudar como coletar evidências de crimes e suas violações, analisar e documentar casos, seguindo metodologias próprias para a investigação de crimes e delitos comuns (Noblett, 1995).

Assim, a computação forense consiste no uso de métodos científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital (ABNT, 2013). Sua aplicação nem sempre é simples, pois trata de coletar e examinar uma evidência que só existe no mundo das ideias (Peck, 2007).

Por evidência digital, entende-se, portanto, a informação armazenada ou transmitida em formatos ou meios digitais (Peck, 2007). Os materiais comprobatórios, na maioria das vezes, são frágeis e voláteis, e por isso requerem a atenção de um experto certificado e experiente, a fim de garantir que possam ser efetivamente isolados e extraídos correta e licitamente. A esse especialista se dá o nome de perito forense em computação. A extração desses materiais pode ser apresentada em tribunais como provas da dinâmica, autoria e materialidade de um crime virtual.

Há, contudo, um problema nessa seara tecnológica. À medida que a tecnologia avança, cria-se grande quantidade de periféricos, nem sempre compatíveis entre si, como celulares *smartphones*, *tablets*, *netbooks*, *notebooks*, *desktops*, servidores, PDA, dentre outros, além de armazenamentos como "nuvem", *pendrives*, HDs

[6] Computação forense é um ramo da ciência forense digital pertencente às evidências encontradas em computadores e em mídias de armazenamento digital.

externos, sistemas RAID etc. Tudo isso integrado à crescente demanda por utilização de redes sociais para uso pessoal e corporativo. Quem hoje não está na *internet*, não existe (Peck, 2007). Assim, quando ocorre um delito por um ou mais desses meios, a importância do uso do procedimento adequado na cena de crime é a diferença entre o sucesso e o fracasso de uma condenação. Pode-se absolver um culpado ou, pior, penalizar um inocente. O modo de coleta e produção da prova é fundamental para a correta aplicação da pena e para a manutenção da justiça (Dorea, 2010). Para tanto, faz-se necessário entender e diferenciar a prova para o meio concreto ou tangível de sua forma para o meio abstrato ou intangível.

3 Evidências digitais e documento eletrônico

É nesse mote que o trabalho se direciona para a composição de uma cadeia de custódia para elementos digitais. Um corpo material se pode tomar ou impor como elemento de prova ou evidência; no mundo abstrato, isso não é possível.

Questiona-se: como fazer para armazenar (custodiar) um *bit*, um sinal elétrico, um fóton? No mundo digital, todas as ideias e dados são informações. Tudo são dados, e estes são armazenados em um formato ininteligível para o ser humano (Peck, 2007).

Um formato digital e codificado segundo a tabela Extended Binary Coded Decimal Interchange Code (EBECDIC), ou a American Standard Code for Information Interchange (ASCII), tem correlação abstrata para um ser humano e é codificado por um computador. Na ciência da computação, tudo são números e tudo são dados (Stuart, 2011; Peck, 2007).

Figura 4 - Exemplo Tabela EBCDIC

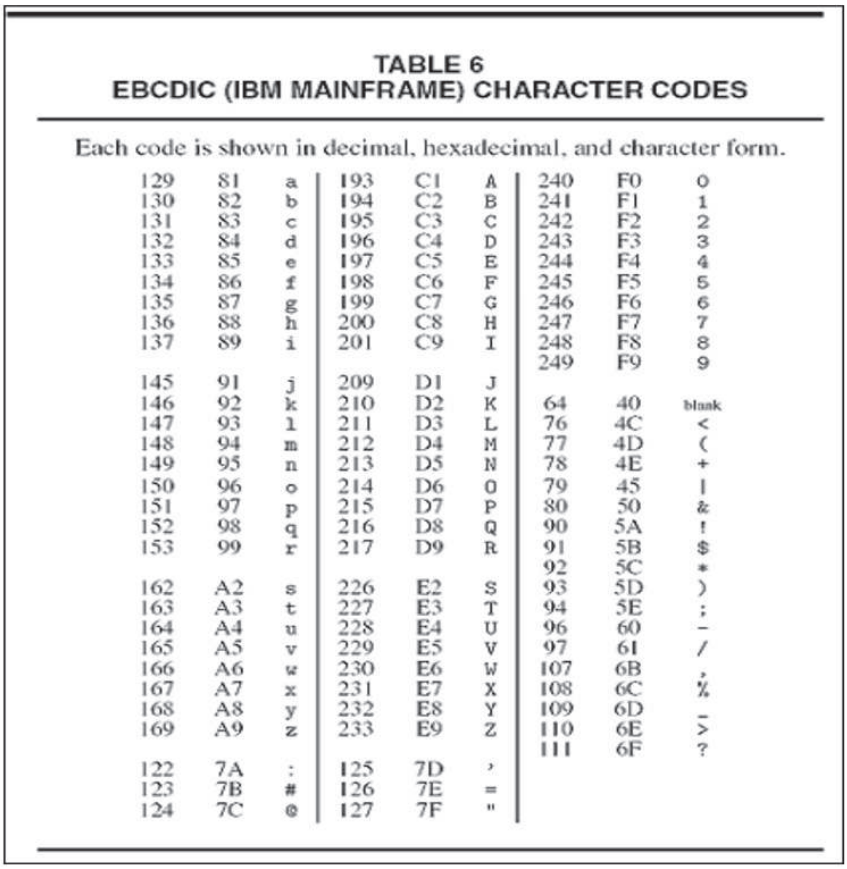


TABLE 6
EBCDIC (IBM MAINFRAME) CHARACTER CODES

Each code is shown in decimal, hexadecimal, and character form.

129	81	a	193	C1	A	240	F0	0
130	82	b	194	C2	B	241	F1	1
131	83	c	195	C3	C	242	F2	2
132	84	d	196	C4	D	243	F3	3
133	85	e	197	C5	E	244	F4	4
134	86	f	198	C6	F	245	F5	5
135	87	g	199	C7	G	246	F6	6
136	88	h	200	C8	H	247	F7	7
137	89	i	201	C9	I	248	F8	8
						249	F9	9
145	91	j	209	D1	J			
146	92	k	210	D2	K	64	40	blank
147	93	l	211	D3	L	76	4C	<
148	94	m	212	D4	M	77	4D	(
149	95	n	213	D5	N	78	4E	+
150	96	o	214	D6	O	79	45	|
151	97	p	215	D7	P	80	50	&
152	98	q	216	D8	Q	90	5A	!
153	99	r	217	D9	R	91	5B	$
						92	5C	*
162	A2	s	226	E2	S	93	5D	)
163	A3	t	227	E3	T	94	5E	;
164	A4	u	228	E4	U	96	60	-
165	A5	v	229	E5	V	97	61	/
166	A6	w	230	E6	W	107	6B	,
167	A7	x	231	E7	X	108	6C	%
168	A8	y	232	E8	Y	109	6D	_
169	A9	z	233	E9	Z	110	6E	>
						111	6F	?
122	7A	:	125	7D	'			
123	7B	#	126	7E	=			
124	7C	@	127	7F	"			

Fonte: Imagem da *internet* (2018).

Figura 5 - Exemplo Tabela ASCII

Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char
0	0000 0000	00	[NUL]	32	0010 0000	20	space	64	0100 0000	40	@	96	0110 0000	60	`
1	0000 0001	01	[SOH]	33	0010 0001	21	!	65	0100 0001	41	A	97	0110 0001	61	a
2	0000 0010	02	[STX]	34	0010 0010	22	"	66	0100 0010	42	B	98	0110 0010	62	b
3	0000 0011	03	[ETX]	35	0010 0011	23	#	67	0100 0011	43	C	99	0110 0011	63	c
4	0000 0100	04	[EOT]	36	0010 0100	24	$	68	0100 0100	44	D	100	0110 0100	64	d
5	0000 0101	05	[ENQ]	37	0010 0101	25	%	69	0100 0101	45	E	101	0110 0101	65	e
6	0000 0110	06	[ACK]	38	0010 0110	26	&	70	0100 0110	46	F	102	0110 0110	66	f
7	0000 0111	07	[BEL]	39	0010 0111	27	'	71	0100 0111	47	G	103	0110 0111	67	g
8	0000 1000	08	[BS]	40	0010 1000	28	(	72	0100 1000	48	H	104	0110 1000	68	h
9	0000 1001	09	[TAB]	41	0010 1001	29	)	73	0100 1001	49	I	105	0110 1001	69	i
10	0000 1010	0A	[LF]	42	0010 1010	2A	*	74	0100 1010	4A	J	106	0110 1010	6A	j
11	0000 1011	0B	[VT]	43	0010 1011	2B	+	75	0100 1011	4B	K	107	0110 1011	6B	k
12	0000 1100	0C	[FF]	44	0010 1100	2C	,	76	0100 1100	4C	L	108	0110 1100	6C	l
13	0000 1101	0D	[CR]	45	0010 1101	2D	-	77	0100 1101	4D	M	109	0110 1101	6D	m
14	0000 1110	0E	[SO]	46	0010 1110	2E	.	78	0100 1110	4E	N	110	0110 1110	6E	n
15	0000 1111	0F	[SI]	47	0010 1111	2F	/	79	0100 1111	4F	O	111	0110 1111	6F	o
16	0001 0000	10	[DLE]	48	0011 0000	30	0	80	0101 0000	50	P	112	0111 0000	70	p
17	0001 0001	11	[DC1]	49	0011 0001	31	1	81	0101 0001	51	Q	113	0111 0001	71	q
18	0001 0010	12	[DC2]	50	0011 0010	32	2	82	0101 0010	52	R	114	0111 0010	72	r
19	0001 0011	13	[DC3]	51	0011 0011	33	3	83	0101 0011	53	S	115	0111 0011	73	s
20	0001 0100	14	[DC4]	52	0011 0100	34	4	84	0101 0100	54	T	116	0111 0100	74	t
21	0001 0101	15	[NAK]	53	0011 0101	35	5	85	0101 0101	55	U	117	0111 0101	75	u
22	0001 0110	16	[SYN]	54	0011 0110	36	6	86	0101 0110	56	V	118	0111 0110	76	v
23	0001 0111	17	[ETB]	55	0011 0111	37	7	87	0101 0111	57	W	119	0111 0111	77	w
24	0001 1000	18	[CAN]	56	0011 1000	38	8	88	0101 1000	58	X	120	0111 1000	78	x
25	0001 1001	19	[EM]	57	0011 1001	39	9	89	0101 1001	59	Y	121	0111 1001	79	y
26	0001 1010	1A	[SUB]	58	0011 1010	3A	:	90	0101 1010	5A	Z	122	0111 1010	7A	z
27	0001 1011	1B	[ESC]	59	0011 1011	3B	;	91	0101 1011	5B	[	123	0111 1011	7B	{
28	0001 1100	1C	[FS]	60	0011 1100	3C	<	92	0101 1100	5C	\	124	0111 1100	7C	|
29	0001 1101	1D	[GS]	61	0011 1101	3D	=	93	0101 1101	5D	]	125	0111 1101	7D	}
30	0001 1110	1E	[RS]	62	0011 1110	3E	>	94	0101 1110	5E	^	126	0111 1110	7E	~
31	0001 1111	1F	[US]	63	0011 1111	3F	?	95	0101 1111	5F	_	127	0111 1111	7F	[DEL]

Fonte: Imagem da *internet* (2018).

Existe a possibilidade de substituir documentos em papel por documentos eletrônicos; estes nada mais são do que sequências de números binários que, reconhecidos e traduzidos pelo computador, representam uma informação. Qualquer arquivo digital contendo textos, sons, imagens ou instruções é um documento eletrônico e tem sua forma original em *bits*, ou seja, não é impresso ou assinado em papel e toda sua cadeia de circulação e autenticidade se dão em sua forma original, ou seja, eletrônica. O original é o que está em *bits*, e o impresso é uma cópia (Peck, 2007). São evidentes as vantagens quanto ao armazenamento, transmissão e recuperação de documentos eletrônicos, se comparadas com as do papel (Brasil, 2009). O termo *documento eletrônico* foi definido, em nosso país, pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001, cuja existência endossa a existência do documento eletrônico no ordenamento jurídico brasileiro.

Em suma, um dado no computador é, em sua base, uma sequência binária de uns e zeros. Em última instância, é essa cadeia que as buscas forenses realizam (Macedo, 2012). São esses dados que têm valor para as pessoas e são esses que deverão ser examinados a fim de produzir prova judicial (Peck, 2007). São elementos voláteis mas perenes, e que dependem sempre de um meio físico para existir. Assim como os escritos de um livro dependem do papel, as informações

digitais dependem de meios computacionais (Peck, 2007). Exemplos de meios de armazenamento de dados ou informação, que são objetivos da busca pericial em um ambiente computacional são (Revistabw, 2018):

a. Dispositivos USB Pen Drive
b. HDD
c. SSD
d. Disquetes
e. Fitas DAT
f. Fitas cassetes
g. CD
h. DVD
i. Memórias Estáticas ROM
j. Cartões de memória SimCard

São dispositivos computacionais compostos de circuitos eletrônicos ou magnéticos, de forma temporária ou permanente, usados para processamento computacional. Servem como armazenamento temporário ou permanente.

4 Coleta e a ordem de volatilidade dos dados em dispositivos digitais

Dado um cenário de um crime, o investigador forense tem árdua tarefa de decidir entre desligar ou não um sistema, e se este é o modo mais eficiente de coletar potenciais vestígios eletrônicos (Wiles, 2007). Há poucos anos, o procedimento da computação forense se resumia a analisar um disco rígido, sem a preocupação com o conteúdo de memória, processos em execução e conexões de rede estabelecidas com outras máquinas. Parecia ser uma verdade imutável.

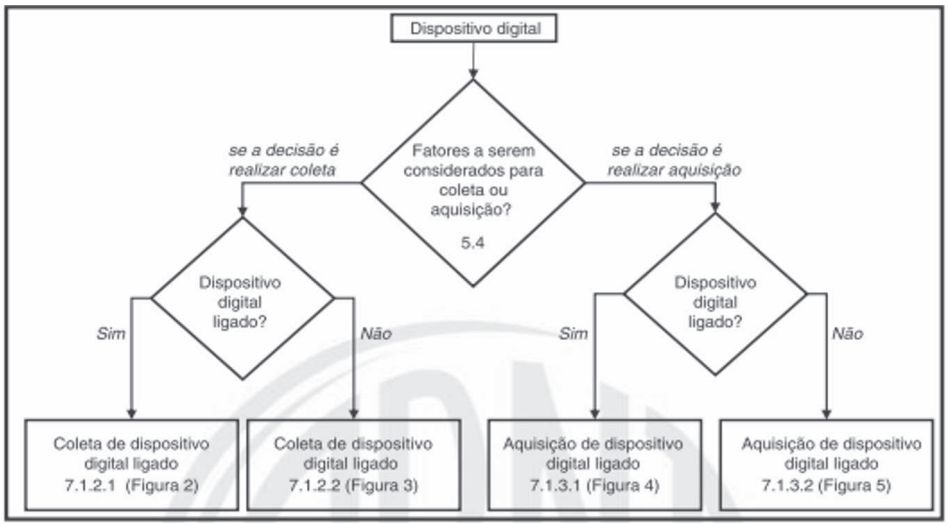
Deve-se, antes tudo, ao examinar um sistema computacional, verificar onde e de que forma os dados estão localizados para o uso da investigação, sendo que se pode obtê-los em dois tipos de memória: a volátil, que perde seu conteúdo ao ser interrompida sua alimentação elétrica e que é a de real interesse para o investigador forense; e a não volátil, que não perde seu conteúdo com a interrupção da alimentação. Discos rígidos são atualmente os mais comumente usados, e a memória *flash* começa a se tornar comum, tanto em dispositivos como em *pendrives*, como também em substituição aos discos rígidos em *notebooks*, *tablets*, telefones celulares e tocadores de música. São, assim, parte do conceito de armazenamento não volátil.

É importante observar o nível de volatilidade ou ordem de volatilidade de um dado digital, em que as informações são armazenadas no sistema periciado ou na mídia questionada, de maneira a sempre iniciar a coleta dos dados mais voláteis

para ou menos voláteis. Caso essa ordem não seja respeitada, haverá um risco de perda e ou alteração dos dados, prejudicando o resultado do trabalho pericial (Farmer, 2007). Por vezes, dependendo do que se busca, é mais vantajoso fazer uma análise com o sistema ligado do que uma análise *post mortem*,[7] ou seja, com o sistema desligado.

O fluxo a seguir ajudará o experto em sua tomada de decisão para execução da coleta ou aquisição da potencial evidência digital.

Figura 6 - Diretrizes para a tomada de decisão para coleta ou aquisição da potencial evidência digital



Fonte: ABNT (2013).

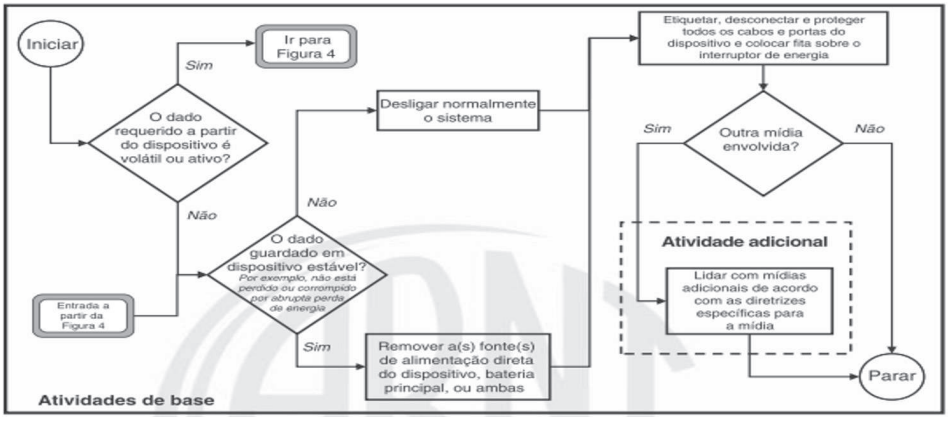
[7] Pode ser descrita como uma espécie de "autópsia" na qual são registradas a descrição do incidente, o seu impacto, as ações que devem ser tomadas para mitigá-lo, as raízes do problema e as ações que devem ser acompanhadas para evitar que o incidente se repita.

Figura 7 - Tempo de vida de algumas mídias de armazenamento de dados

Tipos de Dados	Tempo de Vida
Registradores, memória periférica, caches	Nanossegundos
Memória principal	Dez nanossegundos
Estado da rede	Milissegundos
Processos em execução	Segundos
Disco	Minutos
Disquetes, mídia de backup	Anos
CD-ROMs, impressões	Dezenas de anos

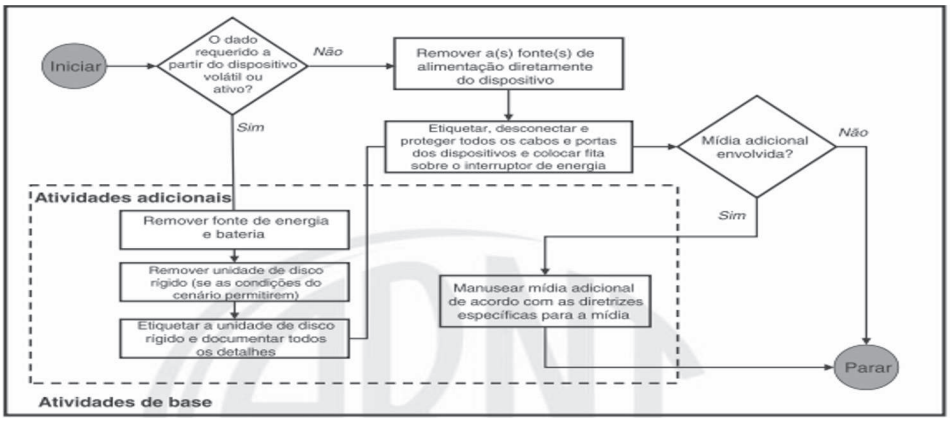
Fonte: Farmer (2007).

Figura 8 - Diretrizes para coleta de dipositivos digitais ligados



Fonte ABNT (2013).

Figura 9 - Diretrizes para coleta de dipositivos digitais desligados



Fonte ABNT (2013).

O maior problema é que análises com o sistema ligado, ou "a quente", podem modificar a estrutura do vestígio a ser examniado, mudando seu conteúdo. A data e hora da criação e modificação de arquivos, chaves de registro (Windows), arquivos de *swap* e conteúdo de memória são modificados quando se faz uma análise de um sistema ligado; portanto, deve-se ter cautela com essa escolha (Macedo, 2012).

Seguindo essa ordem de volatilidade, há uma maior probabilidade de se preservarem os detalhes mais efêmeros que uma mera coleta de dados pode destruir. A RFC 3.227 traz boas práticas para aquisição de evidências digitais, como os estabelecimentos da ordem em que são coletadas, e preza pela coleta inicial das informações voláteis. Um dado volátil é qualquer dado que pode ser perdido com o desligamento do sistema, como uma conexão com um *site* da *internet* que ainda esteja registrado memória RAM.

5 Coleta de evidências digitais

Uma evidência digital é volátil, complexa e que pode ser alterada acidental ou voluntariamente após uma coleta. A ABNT (2013) coloca diretrizes para execução de coletas quando se trata de fazê-las com o dispositivo computacional ligado ou desligado, as quais podem ser caracterizadas como de base ou adicionais. Convém que as atividades de base sejam aplicadas em todas as circunstâncias, enquanto as atividades adicionais sejam aplicadas quando forem relevantes e aplicáveis, dependendo do dispositivo único ou das circunstâncias. São mais bem exemplificados nas figuras 8 e 9.

Assim, para que se possa apontar se uma determinada evidência sofreu alteração em sua integridade, faz-se necessário o estabelecimento de uma cadeia de custódia. Como já exposto, a cadeia de custódia é definida como um processo para manter e documentar cronologicamente uma evidência e deve incluir: nomes ou iniciais dos indivíduos que coletaram as evidências; pessoas ou entidades que, após a coleta, tiveram acesso à evidência; as datas que os itens foram coletados ou transferidos; o órgão e o número do caso; os nomes das vítimas ou suspeitos e, se possível uma breve descrição do caso em tela.

De acordo com Nascimento (2013), no Brasil, o tema ainda é pouco conhecido ou mal compreendido, como não está previsto em lei. Não raro, em muitas ocasiões, os trâmites complexos da cadeia são descumpridos ou tratados inadequadamente, razão dada, talvez pelo desinteresse de ser rigorosamente científica e, outras vezes, por simples ignorância acerca de sua importância ou a aplicação dos métodos adequados.

Não temos, na legislação atual, referencial específico sobre a matéria *cadeia de custódia*. De acordo com Espíndula (2009), o Código de Processo Penal brasileiro determina que a autoridade policial deverá providenciar que não se alterem o estado das coisas e apreender os objetos que tenham relação com o fato – condutas que compõem a cadeia de custódia –, mas não menciona a necessidade de manter uma cadeia de custódia, termo que sequer está presente no código. Para o perito Guliano Giova (2011), o ciclo de vida da evidência digital está se tornando mais complexo, e cada estágio aumenta a probabilidade de uma brecha que viole a cadeia de custódia. O resultado é um cenário de dificuldade crescente para que o Judiciário avalie a evidência e a considere genuína e confiável.

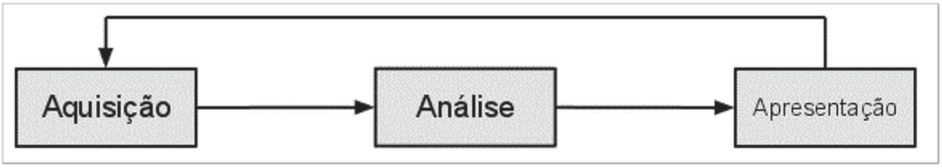
6 Padrões da computação forense e das diretrizes para identificação, coleta, aquisição e preservação de evidências digital

Existem comitês internacionais reconhecidos que tratam e recomendam padronizações e métodos de forense computacional, que foram aprovados pela International Organisation on Computer Evidence (IOCE, 2002) e que formam um guia de boas práticas de procedimentos em forense computacional e da ISO NBR IEC 27.037. Esta trata, por seus domínios, das diretrizes para identificação, coleta, aquisição e preservação de evidências digitais, padronização que originou uma lista de princípios de melhores práticas (ABNT, 2013).

Este trabalho tratará apenas das questões referentes à cadeia de custódia. Entretanto, para um melhor entendimento do processo macros, que podem, para efeitos didáticos, serem divididos em três etapas: aquisição, na qual as evidências são coletadas e catalogadas, via formação inicial da cadeia de custódia; análise,

na qual as evidências são examinadas; apresentação, na qual se mostram os resultados da perícia.

Figura 10 - Fases do processo de perícia forense computacional



Fonte: Imagem da *internet* (2018).

Como demonstrado no diagrama da Figura 10, a forense computacional compreende identificação, conservação e análise da informação, seja ela armazenada, seja transmitida, seja produzida por um sistema computacional. Um de seus principais objetivos é realizar investigações de forma organizada e estruturada, com padrões e metodologias que auxiliem no processo para descobrir detalhes específicos dos crimes, apresentando resultados que possam ajudar também no processo criminal em si. Por isso, ressalta-se o dever de examinar cada fragmento dos dados disponíveis, para que a intenção do invasor de esconder ou criar falsas provas seja descoberta (Farmer, 2007; Texeira, 2009).

7 Cadeia de custódia com suporte ao artigo 158-A do CPP

Como anteriormente explicado, o processo de coletar evidências digitais, dada a sua volatilidade, deve obedecer a métodos ligeiramente diferente das coletas de material concreto. Alguns modelos foram propostos para manter uma cadeia de custódia (Carrier, 2004), como *softwares* especificamente criados para procedimentos forenses informatizados e que podem, adicionalmente, fornecer melhor descrição das evidências, auditoria automática, assim como gerar *hashs*[8] criptográficos para futura verificação da sua integridade.

A fim de manter uma cadeia de custódia, dentre outros fatores menos relevantes, pode haver variações em função da legislação local ou de um determinado país na aplicação desses modelos. Mas o importante é que eles devem ser capazes de conhecer plenamente as personagens envolvidas e suas atividades em todo processo forense. São procedimentos que permitem ao investigador recuperar ou

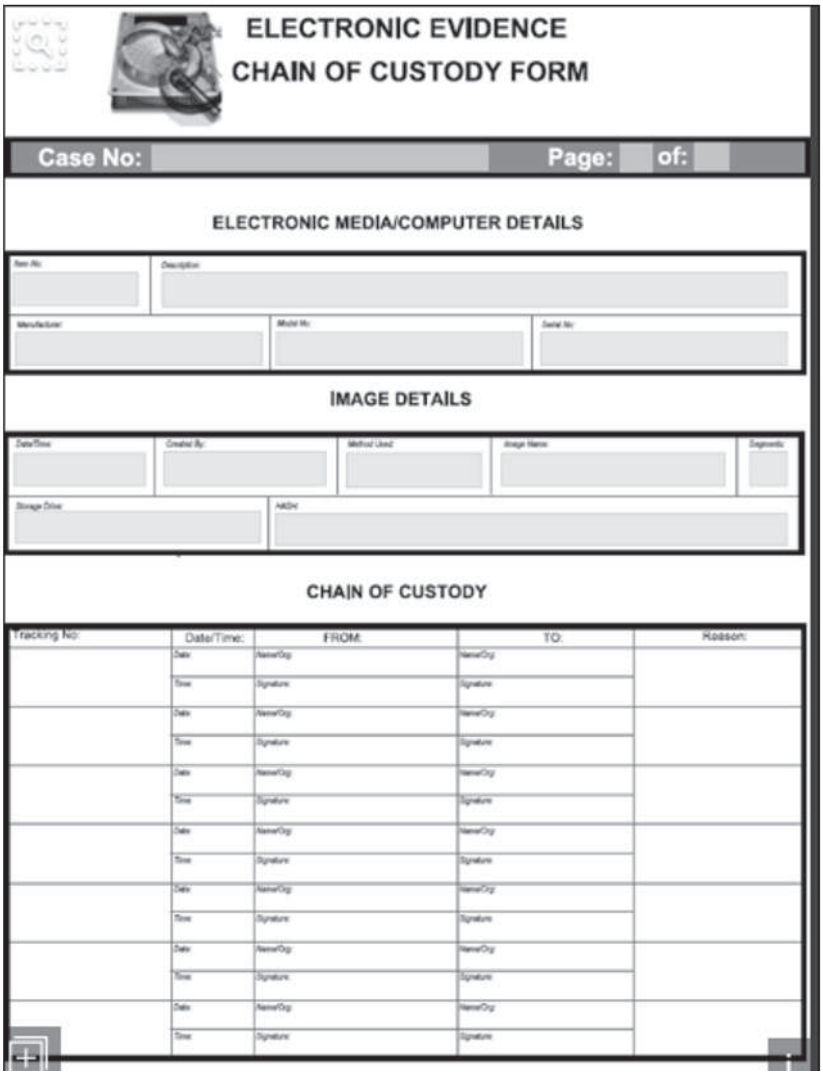
[8] Uma função de dispersão criptográfica, ou função *hash* criptográfica, é uma função *hash* considerada praticamente impossível de inverter, isto é, de recriar o valor de entrada utilizando somente o valor de dispersão. Essas funções *hash* unidirecionais têm sido chamadas de "operários da criptografia moderna".

restaurar dados dos dispositivos computacionais envolvidos em atos ilícitos e usá-los como evidências em uma investigação criminal, civil ou de qualquer outra esfera judicial (Noblett, 2000).

Tais procedimentos requerem robustez tecnológica para assegurar que todas as informações probatórias sejam devidamente recuperadas e possam ser novamente periciadas a qualquer tempo. Ainda mais, as evidências digitais devem ser tratadas de forma tal que se possa garantir que nada na fonte da evidência original seja alterado. Quando se versa sobre forense computacional, fala-se de boas práticas, com métodos e procedimentos confiáveis, e de uma ciência que trabalha com evidências voláteis que existem apenas em circuitos eletrônicos.

A ABNT (2013), em seu Capítulo 5.3, detalha os requisitos para o manuseio da evidência digital; no Capítulo 5.4, do processo de manuseio e coloca dois princípios que tratam da relevância e da confiabilidade. Explica ainda que os materiais podem ser recolhidos por meio de aquisição e ou de atividade de coleta, que devem ser feitas e acondicionadas com equipamentos e formulários específicos, como os apresentados pelas figuras 11 e 12.

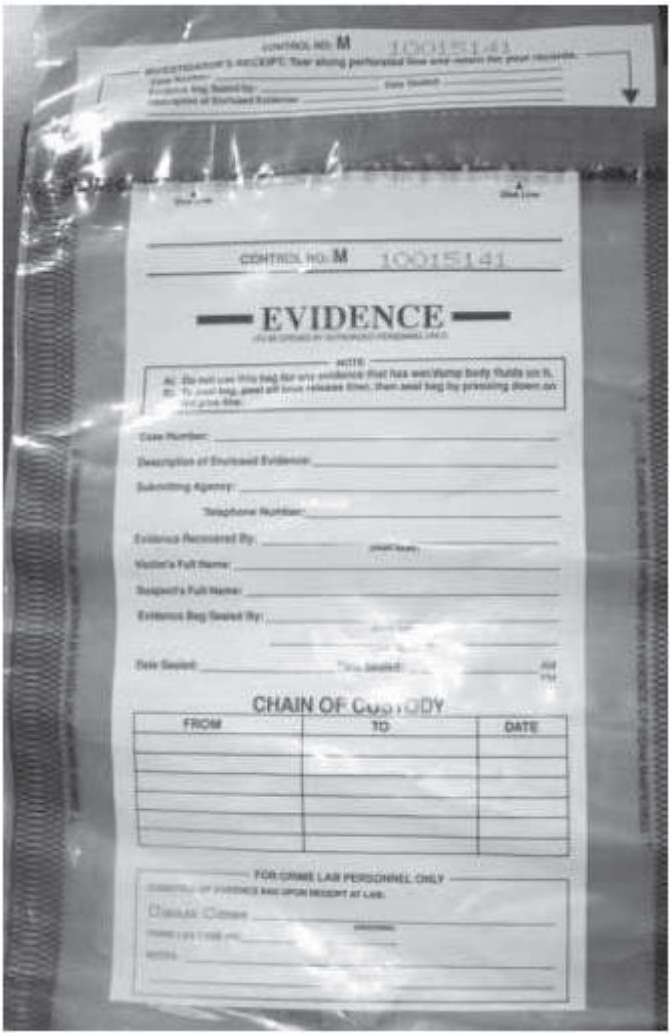
Figura 11 - Formulário de cadeia de custódia



Fonte: Imagem da *internet* (2018).

Já os subitens 5.4.2 e 5.4.3 tratam, respectivamente, das etapas de identificação, coleta e acondicionamento (custódia) adequados, objetivando dar valor probatório.

Figura 12 - Saco de evidências



Fonte: Macedo (2012).

Infelizmente, não existe um formulário padronizado ou saco de custódia para evidências específico para coleta digital, pois, como esclarecido, as evidências digitais estão armazenadas em um dispositivo eletroeletrônico-mecânico, e fica ao livre-arbítrio do perito como coletá-la e identificá-la. Como o tema deste trabalho se assenta na validade das provas digitais pela correta aquisição e catalogação de cadeia de custódia, precisamos delimitar a real necessidade de as provas terem valor jurídico probatório para ajudar o juízo de convicção a partir delas. Umas das formas de propor tal garantia versa sobre a criação e manutenção de uma cadeia

de identificação, usando-se procedimento e material adequado, corretamente formulado, preenchido e custodiado. A prova digital é perene e requer outros cuidados, como proteção contra interferência eletromagnética, calor e umidade. Os documentos digitais possuem certas particularidades bastantes relevantes quando falamos sobre sua validade, e consequentemente sua força probatória (Lessa, 2009). Portanto, acondicioná-los de forma correta a fim de que tenha validade jurídica é fundamental para a manutenção da boa ordem pericial.

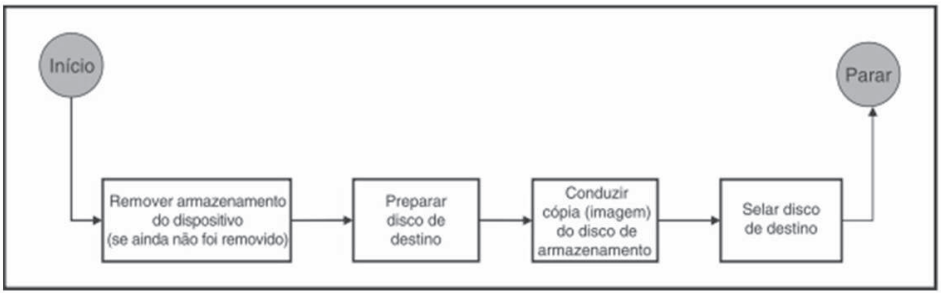
8 O processo de investigação

Após a fase da coleta e da correta formatação da cadeia de custódia, inicia-se o processo de exame e análise, também chamado de processo investigativo. O procedimento para realizar uma perícia pode variar dependendo do que deve ser periciado e em quais condições as evidências se encontram. Este artigo não intenta ser um tutorial forense e somente apresentará o descritivo das principais etapas de uma rotina forense em meios digitais, norteada pelas *Diretrizes para identificação, coleta, aquisição e preservação de evidência digital* (ABNT, 2013).

8.1 Aquisição

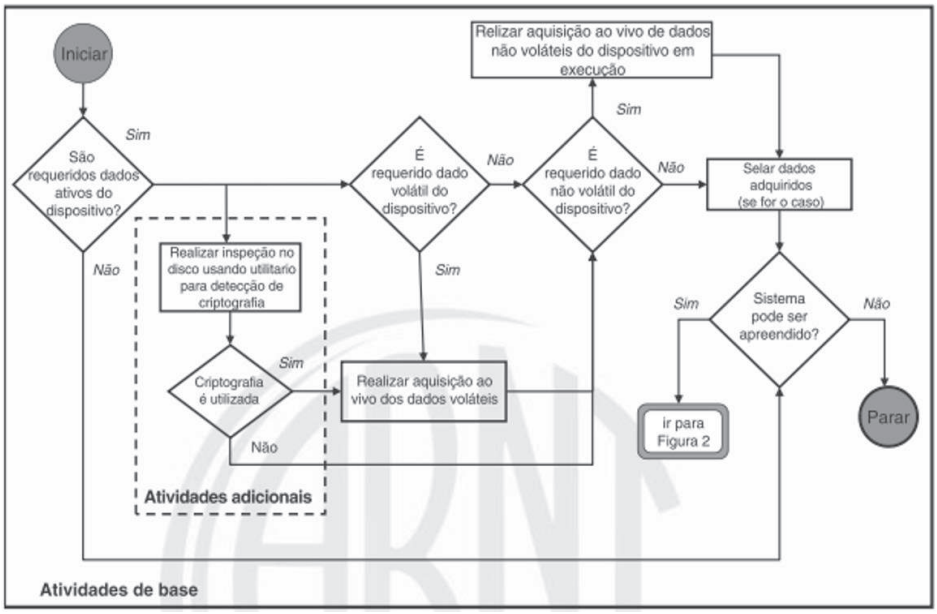
A aquisição é a etapa mais crítica do processo, durante a qual se deve garantir que a integridade das evidências, como o uso de bloqueadoras de escrita para que atributos do MAC Time não se alterem (Farmer, 2007). Os MAC Times são metadados que indicam os horários de acesso de um arquivo, cuja análise é de extrema importância para uma investigação.

Figura 13 - Diretrizes para a aquisição de dispositivos digitais desligados



Fonte: ABNT (2013).

Figura 14 - Diretrizes para a aquisição de dispositivos digitais desligados



Fonte: ABNT (2013).

8.2 Preservação

Para este trabalho, a preservação é a etapa mais significativa, pois permite que uma evidência seja usada como formatação de prova com peso processual jurídico. Como já dito, é necessário que a perícia realizada nas evidências possa ser repetida a qualquer tempo. Para computação forense, a preservação do material questionado trata do simples fato de copiar ou cloná-lo, desde que se possa garantir sua cadeia de custódia. Outro atributo importante nessa etapa é a geração de validações por assinatura *hash* que permita, se questionado, a verificação de sua integridade. Preservar os dados significa garantir o bloqueio de dados antes da cópia *bit* a *bit*, impedindo que a mídia original sofra algum tipo de alteração durante o processo de aquisição (ABNT, 2003).

8.3 Identificação

Todas as evidências recolhidas para análise devem ser detalhadamente descritas em um documento denominado *cadeia de custódia*, que deve ser mantido junto do material questionado.

8.4 Extração

Segundo Galvão (2009), a extração dos dados deve ser feita após a coleta, para posterior análise. Implica o processo de retirar das mídias periciadas as informações disponíveis e fundamentais para o caso em tela, a exemplo da estrutura do sistema de arquivos de um sistema, arquivos de sistemas, usuários ativos, dispositivos acessados, navegação na *internet*, *drivers* compartilhados ou registros com as informações de MAC Times dos arquivos, para determinar se algum deles foi alterado.

8.5 Recuperação

A recuperação é processo centrado na busca por dados removidos total ou parcialmente, propositalmente ou não. Trata de buscar por dados deletados e tentar recuperá-los. Os ferramentais forenses disponíveis possibilitam a realização do processo, executando uma análise de blocos não alocados do sistema de arquivo na busca de vestígios de arquivos deletados que possam ser recuperados. Tais vestígios podem ser recuperados até que algum outro arquivo sobrescreva o bloco onde ele se encontra. Com sorte, o experto forense logrará recuperar grande parte do que busca em uma mídia questionada.

8.6 Exame e análise

O exame e análise é etapa que analisa os dados extraídos e recuperados pelo perito. Em virtude da criticidade, é a fase que mais demanda atenção e tempo pericial. Nela o perito tentará recriar o incidente e formalizar sua dinâmica, que é relatar o como o fato ocorreu (quais arquivos foram apagados ou copiados, por quais *sites* o investigado navegava, como e com quem mantinha contatos etc.). Galvão (2009) volta a atenção para os cuidados que devem ser tomados nessa fase, que são proporcionais ao volume de dados analisados, já que nem sempre as evidências são explícitas.

8.7 Apresentação

O resultado do trabalho pericial se consubstancia num relatório chamado *laudo pericial em informática*, o enquadramento das evidências dentro do formato jurídico. Esse documento deve apresentar as conclusões do perito em linguagem clara, direta e objetiva e será utilizado para formatar valor em julgamentos e em

sentenças judiciais. Deve conter uma estrutura similar à apresentada pelo CPC,[9] além da metodologia, técnicas e *softwares* utilizados pela perícia, bem como todas as cadeias de custódias usadas por todas as evidências coletadas e analisadas. O laudo deve conter: finalidade da investigação; autores; resumo do caso; relação de evidências analisadas e seus detalhes; metodologia; ferramentais; conclusão; anexos; apêndices e glossário, se necessário.

9 Projeto de Lei nº 4.939/2020

Atualmente a doutrina define como prova digital todo elemento extraído ou armazenado em meio digital apto a provar ocorrência ou inocorrência de fato. O Projeto de Lei nº 4.939/2020 é uma proposição legislativa apresentada à Câmara dos Deputados do Brasil que dispõe sobre as diretrizes do Direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. A Lei nº 13.964/2019 não abarca com detalhes a coleta e preservação de artefatos digitais, as quais devem ser, no que couber, adaptadas à realidade de provas digitais, pois não foram pensadas para isso como a PL nº 4.939/2020.

Portanto, o quanto se pode, devem-se utilizar as etapas previstas no artigo 158-B e subsidiariamente aplicar os passos e métodos descritos no PL nº 4.939/2020.

10 Conclusão

Em que pese a Lei nº 13.964/2019 introduzir no CPP nos artigos 158-A e 158-B os 10 procedimentos ou etapas para a criação da cadeia de custódia, estas não abarcam a totalidade das formas esperadas para aplicação dos mesmos procedimentos a serem aplicados em artefatos eletrônicos. Isso seria em parte resolvido com a absorção do Projeto de Lei nº 4.939/2020, que trata das diretrizes do Direito da Tecnologia da Informação e das normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências.

O objetivo da investigação forense é encontrar fatos e, por meio deles, recriar a verdade sobre o acontecimento. O examinador acessa a verdade sobre um acontecimento, descobrindo e expondo os vestígios que foram deixados no sistema, os quais podem ser transformados em provas que, periciadas, recriam um passado. Analisadas e processadas pelo homem, portanto, são propensas a erros e enganos.

[9] Art. 473 do CPC.

Destarte, a preocupação com a custódia dos vestígios (corpo de delito) é um dos principais requisitos avaliadores da competência e qualidade do serviço pericial. O trabalho demonstra a necessidade da validação da prova e do meio como ela foi obtida e custodiada, o qual se dá por um processo chamado de *cadeia de custódia*. Esta deve ser vista como um critério de aceitação ou desentranhamento da prova processual e item de análise em todos os processos judiciais, podendo ser replicada a qualquer tempo. Assim, este artigo finaliza demonstrando que a prova digital tem particularidades incomparáveis com outros meios de produção de prova, e que alguns dos elementos que a fazem valer em um tribunal são a derivação e a formatação de sua cadeia de custódia.

A look at computer forensic expertise and the application of the collection and preservation of evidence in digital environments and the formation of the chain of custody according to ISO 27.037, Law No. 13.964 and PL No. 4939/2020 driven by the annulment of evidence obtained in Odebrecht systems in all spheres and for all actions by the STF

Abstract: The chain of custody contributes to the validation of expert evidence obtained, examination and presentation in a work that is embodied in a report called an expert report. The formatting of a test is essential to establish the correct legal process and so that it can be replicated or reproduced at any time according to a scientific method that is accepted by the academic community and has legal value. The responsibility for maintaining fairness and procedural integrity is shared by all parties involved in the dispute, with attention to the judicial expert, as it is on their shoulders that the responsibility for obtaining evidence and maintaining the chain of custody falls. The need for standardized operational procedures is fundamental so that, in the face of questions presented by courts and employers, expert evidence remains robust and reliable, based on the magistrate's free conviction in his sentence. Finally, Bill No. 4,939/2020 deals with the guidelines of Information Technology Law and the rules for obtaining and admissibility of digital evidence in investigation and proceedings, in addition to other exceptions. At the time of writing this article, however, it has not been voted on or incorporated into the Brazilian legal system. On September 6, 2023, during "Operation Spoofing", Minister Dias Toffoli (STF) granted the measure that nullifies any and all evidence obtained from the Drousys and My Web Day B systems, used based on the leniency agreement signed by Odebrecht, within the scope of "Operation Lava Jato". The decision attacked on the merits complies with Complaint No. 4.3007 and makes the evidence and other elements obtained from this agreement definitively useless, with *erga omnes* effects, in any scope or degree of jurisdiction based on proven elements. The methodology used in this work, widely accepted and disseminated, is the collection and study of theoretical references, with analysis of ABNT regulations. Ultimately, it aims to provide legal support for the need to collect evidence from electronic devices and collaborate with experts in the field of computer forensics to show that digital evidence has particularities that are incomparable with other means of producing evidence, and that some elements to enforce in a court of law are the derivation and formatting of its chain of custody.

Keywords: Chain of custody. Graphotechnical expertise. Law. evidence.

Referências

ABNT. *NBR 27.037*: diretrizes para identificação, coleta, aquisição e preservação de evidencia digital. Rio de Janeiro: [*s. n.*], 2013.

BRASIL. *Certificados Eletrônicos e Assinaturas Digitais*. Disponível em: http://cert.oab.org.br/cert_assin.htm. Brasília, DF: ICP-OAB, 2009.

BRASIL. Decreto-Lei nº 3.689. Código de Processo Penal. *Diário Oficial da União*: Brasília, DF, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 5 mar. 2018.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. Diagnóstico da Perícia Criminal. *Gov.br.*, Brasília, DF, 2012. Disponível em: http://www.justica.gov.br/sua-seguranca/seguranca-publica/senasp-1/pops-de-pericia-verso-para-internet.pdf. Acesso em: 5 mar. 2018.

CARRIER, B.; D. SPAFFORD, D. An Event-Based Digital Forensic Investigation Framework. *Digital Forensic Research Workshop*, [*S. l.*], 2004.

CHASIN, A. A. M. Parâmetros de confiança analítica e irrefutabilidade do laudo pericial em toxicologia Forense. *Revista Brasileira de Toxicologia*, [*S. l.*], v. 14, n. 1, p. 40-46, 2001.

DOREA, L. E. *Criminalística*. 4. ed. São Paulo. Millenium Editora. 2010.

ESPÍNDULA, A. *Perícia criminal e cível*: uma visão geral para peritos e usuários da perícia. 3. ed. São Paulo. Millenium Editora. 2009.

FARMER, D.; VEBEMA, W. *Perícia forense computacional*. Teoria e prática aplicada. São Paulo: Pearson Prentice Hall, 2007.

GALVÃO, R. *Computer Forensics with The Sleuth Kit and The Autopsy Forensic Browser*, [*S. l.*], [2018]. Disponível em: http://www.ijofcs.org/V01N1-P05%20-%20Computer%20Forensics%20with%20the%20Sleuth%20Kit.pdf. Acesso em: 5 mar. 2018.

GIOVA, G. Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems. *International Journal of Computer Science and Network Security*, [*S. l.*], v.1 1, n. 1, 2011.

IOCE. *Guidelines for Best Practice in the Forensic Examination of Digital Technology*. [*S. l.*]: IOCE, 2002.

JÚNIOR, E. F. A cadeia de custódia e a prova pericial. *Jus*, [*S. l.*], 2 abr. 2012. Disponível em: https://egov.ufsc.br/portal/conteudo/cadeia-de-cust%C3%B3dia-e-prova-pericial. Acesso em: 5 mar. 2018.

LESSA, B. M. A invalidade das provas digitais no processo judiciário. *Conteúdo Jurídico*, Brasília, DF, 2 dez. 2009. Disponível em: http://www.conteudojuridico.com.br/?artigos&ver=2.25613&seo=1. Acesso em: 5 mar. 2018.

MACEDO, D. A aquisição e preservação dos dados na forense computacional. *In:* MACEDO, D. *Diego Macedo*. [*S. l.*], 2012. Blog disponível em http://www.diegomacedo.com.br/a-aquisicao-e-preservacao-dos-dados-na-forense-computacional/. Acesso em: 5 mar. 2018.

NOBLETT, M. G.; L. A. PRESLEY. Recovering and Examining Computer Forensic Evidence. *Digital Evidence: Standards and Principles. Forensic Science Communications*, [*S. l.*], v. 2, n. 2, Apr. 2000.

NOBLETT, M. G. Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence. *In:* INTERPOL FORENSIC SCIENCE SYMPOSIUM, 11., 1995, Lyon. *Proceedings* [...]. Boulder: The Forensic Sciences Foundation Press, 1995.

NASCIMENTO, L. J. M.; SANTOS, M. V. F. D. L. Cadeia de custódia. *Revista Científica de Polícia Técnica da Secretaria de Segurança Pública da Bahia*, [*S. l.*], ano 2, n. 6, dez. 2005.

PECK, Patrícia P. *Direito Digital*. 2. ed. São Paulo: Saraiva Editora. 2007.

REVISTABW. Arquitetura de computadores: dispositivos de memória e armazenamento. Revista Brasileira de Web. Tecnologia. Disponível em http://www.revistabw.com.br/revistabw/memoria/. Acesso em: 6 abr. 2018.

SILVA, J. A. *Curso de Direito Constitucional positivo*. 32. ed. São Paulo: Malheiros, 2009.

STUART, B. L. *Princípios de sistemas operacionais*: projetos e aplicações. São Paulo. Cengage Editora, 2011.

TEIXERA, A. *Perícia forense de rede*: teoria e prática. 2009. Trabalho de Conclusão de Curso (Pós-graduação em Administração de Redes Linux) – Faculdade de Ciências da Computação, Universidade Federal de Lavras, Lavras, 2009. Disponível em: http://www.ginux.ufla.br/files/mono-AdrianaTeixeira.pdf. 2009. Acesso em: 6 abr. 2018.

WILES, J.; CARDWELL, K.; REYES, A. The best damn cybercrime and digital forensics. *Book Period*, [*S. l.*], 2007.

ANEXO A - Competências essenciais e descrição das competências. ABNT NBR ISSO/IEC 27037:2013. Exemplo de definição de competências (ABNT, 2013)

Nº	Habilidades fundamentais	Descrição das habilidades fundamentais	Descrição de competências		
			Conscientização (1)	Conhecimento (2)	Habilidade (3)
1	Identificação da evidência digital	Caracterizar dispositivo digital, componentes, informações que podem auxiliar a investigação e leis relevantes para manuseio da potencial evidência digital e crimes cibernéticos. Identificar requisitos de ferramentas para coleta e aquisição de dados e dispositivos e avaliação de riscos.	Uso geral de TI e administração de múltiplos tipos de dispositivos de TI e dispositivos de rede; procedimentos investigativos no cenário do crime; determinação do estado do dispositivo; avaliação da informação como evidência; dispositivos e informação relacionados a redes forenses.	Registros e configuração da aplicação/ identificação do sistema e aplicação de registros de entradas, incluindo registros de entradas em *email, web*, registros de acessos, arquivos de senhas, arquivos *sysconfig*, informação de IP local; funcionalidade do dispositivo e dependências; habilidade para compreender impactos sobre evidências voláteis e não voláteis.	Análise especial; interpretação de registros para detecção de intrusão na identificação de outros sistemas afetados (algumas jurisdições requerem confirmação da presença da evidência antes da coleta); identificar senhas necessárias para os respectivos dispositivos antes da coleta; identificar diagrama de rede e mecanismos de controles de acessos para compreender as dependências; endereços de *link* de IP e endereços de *MAC* para confirmação do dispositivo.

Nº	Habilidades fundamentais	Descrição das habilidades fundamentais	Descrição de competências		
			Conscientização (1)	Conhecimento (2)	Habilidade (3)
2	Coleta da evidência digital	Requisitos de ferramentas e implementação de acondicionamento de evidência digital, proteção contra ameaças ambientais. Áreas protegidas incluem segurança da informação.	Segurança na coleta de dados gerais; princípios e estrutura das ferramentas básicas; determinar o melhor método de coleta para preservar ao máximo a informação relevante para o incidente.	Formular e executar o processo de coleta; coletar evidência; gerar documentos probatórios; cadeia de custódia da evidência; processo de controle de qualidade da evidência; entrevista com suspeitos.	Otimização do processo de coleta; documentar a evidência que não é possível que seja adquirida devido a várias restrições; coletar senhas, chaves, *dongles*, e outras informações necessárias para conduzir a análise em laboratório.
3	Aquisição da evidência digital	Aplicar os requerimentos da aquisição da potencial evidência digital na forma lógica, assegurando a repetibilidade, auditabilidade, reprodutibilidade e justificabilidade. Áreas abrangidas são a aquisição realizada sobre um sistema ligado, a aquisição realizada sobre um sistema desligado e rede forense.	Compreender a informação disponível nos dispositivos digitais, bancos de dados, documentos gerados pelo sistema, dados gerados pelo usuário e dados voláteis; estruturas de arquivos dos sistemas Unix e Windows e aplicações; ter ciência dos impactos sobre dados voláteis.	Saber como determinar requisitos para armazenamento; executar procedimentos de aquisição de imagens (por exemplo, aquisição de mídia de armazenamento parcial e integral); aquisição realizada sobre um sistema ligado, aquisição realizada sobre um sistema desligado; geração de valor de *hash*.	Habilidade para conduzir aquisição de mídia de armazenamento digital incluindo RAID, bancos de dados, aplicações e dispositivos miniaturizados; compreender dependências e impactos sobre diferentes métodos de aquisição.

Nº	Habilidades fundamentais	Descrição das habilidades fundamentais	Descrição de competências		
			Conscientização (1)	Conhecimento (2)	Habilidade (3)
4	Preservação da evidência digital	Aplicar e avaliar os requerimentos para preservação da potencial evidência digital, compreender fatores e parâmetros que influenciam a sua exatidão. Áreas abrangidas são a metodologia, manutenção da cadeia de custódia, manuseio de dispositivos de computador e manuseio de mídias digitais armazenadas.	Compreender as exigências e procedimentos para manutenção da cadeia de custódia contra requerimentos legais; impactos ambientais tais como umidade, temperatura e choques em direção ao dispositivo digital; compreender as opções de acondicionamento, requisitos de transporte e armazenamento.	Saber como gerar documentos da evidência auditáveis; definir parâmetros para os documentos; segurança da informação, ameaças, vulnerabilidades controles da evidência digital.	Aplicar medidas para proteger a evidência digital sob a forma de grandes dispositivos para dispositivos miniaturizados portáteis; procedimento para documentar detalhes da evidência.

1	Conscientização – Reconhecer, identificar – perguntar quando houver necessidade de auxílio
2	Conhecimento – Adquirir por meio de instrução formal ou trabalho em equipe. Contribuir, participar – fazer com auxílio
3	Experiência – Experiência comprovada por meio da aplicação no ambiente de trabalho. Trabalhos sem supervisão. Aplicar, demonstrar – fazer sem auxílio.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

CAPOZZI, Ricardo Andrian. Um olhar sobre a perícia forense computacional, a aplicação da coleta, a preservação de provas em ambientes digitais e a formação da cadeia de custódia, segundo a ISO 27.037, a Lei nº 13.964 e o PL nº 4939/2020, impulsionado pela anulação de provas obtidas em sistemas da Odebrecht em todas as esferas e para todas as ações do Supremo Tribunal Federal (STF). *Revista Fórum Trabalhista – RFT*, Belo Horizonte, ano 13, n. 53, p. 123-152, abr./jun. 2024.