v. 9, n. 2, p. 134-138, 2020
ISSN 2237-9223

REVISTA BRASILEIRA DE CRIMINALÍSTICA

DOI: http://dx.doi.org/10.15260/rbc.v9i2.463

A Importância da Cadeia de Custódia na Computação Forense

R.W.R Carvalho [a,*]

[a] *Associação Nacional dos Peritos em Computação Forense (CE), Brasil*

**Endereço de e-mail para correspondência: romullo2010@gmail.com. Tel.: +55-85-988405936.*

Recebido em 05/03/2020; Revisado em 21/05/2020; Aceito em 04/06/2020

Resumo

Neste artigo apresento uma visão geral sobre o documento de Cadeia de Custódia no âmbito de evidências informáticas. Com base no Código de Processo Penal e boas práticas do Perito Forense é disposto um modelo de formulário de cadeia de custódia que pode ser utilizado para documentar e acompanhar a evidência.

Palavras-Chave: Cadeia de custódia, evidência, computação forense.

Abstract

In this article I present an overview about the Chain of Custody document within the scope of computer evidence. Based on the Code of Criminal Procedure and Good Practices of the Forensic Expert is arranged a model of chain of custody form that can be used to document and monitor the evidence.

Keywords: Template; Chain of custody, evidence, forensic computing.

1. INTRODUÇÃO

Aqui realizamos uma análise sobre o formulário de cadeia de custódia, bem como a sua origem no ato da coleta das evidências, seu armazenamento e análise. Com o foco nas evidências digitais, essa análise leva em consideração não apenas o dispositivo físico, mas os dados que estão gravados na memória de cada evidência.

Este artigo visa dar uma compreensão geral sobre o documento de cadeia de custódia, partindo do momento da coleta até o descarte da evidência. Apresentando também referências do Código de Processo Penal para embasar e sustentar a temática abordada neste presente artigo.

As seções nas quais o trabalho possa ser enquadro são as seguintes:

- Significados
- Importância
- Coleta e contaminação
- Análise
- Modelo
- Código de Processo Penal

2. SIGNIFICADOS

Apresento uma explanação dos significados dos termos utilizados neste artigo.

2.1. Cadeia

Série de ações, fatos ou fenômenos, em geral da mesma natureza, que ocorrem de forma sucessiva ou que podem ser entendidos como etapas de um fenômeno ou sistema mais abrangente; série ininterrupta de coisas, fatos ou objetos semelhantes; continuidade, encadeamento, sucessão.

2.2. Custódia

Ato de guardar, preservar ou proteger; guarda ou detenção de coisa alheia, que se administra e conserva até a entrega ao seu dono legítimo.

2.3. Função de Hash

Algoritmo que gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é

a transformação de uma grande quantidade de informações em uma pequena sequência de bits (hash). Esse hash altera se um único bit da entrada for alterado, acrescentado ou retirado

3. IMPORTÂNCIA

Na formação do conjunto dos elementos probatórios, a cadeia de custódia é de extrema importância, já que tem como principal objetivo, preservar as informações coletadas, possibilitando a documentação e a ordem cronológica das evidências, quem foram os responsáveis por seu manuseio, podendo apresentar a rastreabilidade da evidência coletada.

A cadeia de custódia exige o estabelecimento de um procedimento regrado e formalizado, documentando toda a cronologia existencial daquela evidência, para permitir a posterior validação em juízo.

A preservação da cadeia de custódia exige grande cautela por parte dos agentes do estado, da coleta à análise, de modo que se exige o menor número de custódios possível e a menor manipulação do material. O menor número de pessoas manipulando o material faz com que seja menos manipulado e a menor manipulação, conduz a menor exposição. Expor menos é proteção e defesa da credibilidade do material probatório.

O Perito Criminal deve sempre observar e zelar pela cadeia de custódia de todos os vestígios recolhidos no local de crime, registrando em papel próprio os dados relativos à coleta, individualizando-os e lacrando-os em embalagens adequadas à natureza do vestígio (caixas, sacos, embalagens, latas, etc.) para serem encaminhados a outros exames.

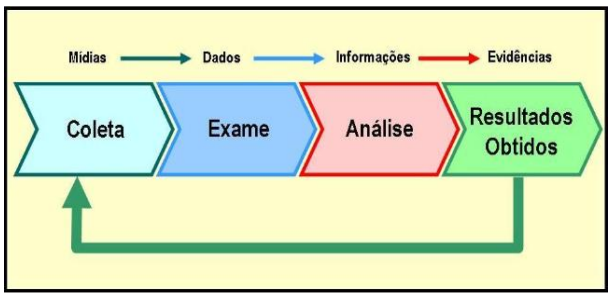


Figura 1. Etapas da investigação.

4. COLETA E CONTAMINAÇÃO

A idoneidade dos vestígios para os posteriores exames está diretamente ligada à adequada coleta, registro, acondicionamento e transporte, que garantirão o êxito dos resultados e, posteriormente, a cadeia de custódia.

Cadeia de custódia se refere ao registro sobre a coleta, posse, manuseio e transferência de evidências físicas ou digitais. Todo o caminho percorrido desde o nascimento de uma evidência até o seu descarte precisa estar devidamente documentado.

As evidências no meio digital representam as informações armazenadas ou transmitidas eletronicamente na forma de bits que podem ser invocadas em juízo, como e-mails, tráfegos de rede, notícias, perfis, fotos, vídeos, áudios, documentos, planilhas e demais arquivos armazenados em dispositivos digitais, como computador, pendrive, celular ou mesmo nas nuvens.

Para a coleta de evidências digitais deve ser calculado o hash da mídia, para fins comparativos com o hash calculado na coleta, após manuseio da mesma da evidência e cópias forenses.

4.1. Quebra da cadeia de custódia

Quando a evidência possui uma cadeia de custódia documentada seguindo os padrões, porém em algum momento houve uma interrupção no registro da cadeia de custódia, ou que o hash nela encontrado não condiz com o que fora anteriormente computado na coleta.

Falhas na cadeia de custódia podem desqualificar e desentranhar evidências de processos seja cível ou criminal. Um simples detalhe pode jogar no lixo todo o trabalho realizado ou modificar radicalmente o rumo de um processo.

A eventual quebra da cadeia de custódia importa, portanto, na ilicitude da prova a que se refere aquele conjunto de atos. Deverá o magistrado, portanto, reconhecer a sua ilicitude e determinar o consequente desentranhamento dos autos. Sem dúvida, será necessário que se pronuncie também acerca da extensão da ilicitude quanto a eventuais provas derivadas.

Somente por ordem dos Peritos Criminais outras pessoas poderão ter acesso à área isolada, cabendo medidas coercitivas no sentido de impedir que pessoas estranhas adentrem ao local isolado (CPP, Art. 6o, inciso I).

4.2. Ausência da cadeia de custódia

Quando não há a existência de nenhuma cadeia de custódia, deixando as evidências sem documentação, identificação, catalogação e/ou prova de manuseio, guarda análise, ou uso. Fazendo com que a evidência possa ter sua integridade e confiabilidade questionada perante o juiz, tornando passível de nulidade.

4.2. Ilicitude da evidência

Durante a Operação Ouro Verde, deflagrada pela Polícia Federal no (Rio Grande do Sul) para investigar ilícitos decorrentes da evasão de divisas. Nas diligências policiais, houve a apreensão do notebook cujo disco

rígido continha os arquivos em que estavam descritas as supostas operações da organização, peça-chave para o oferecimento da denúncia. Ocorre que antes do espelhamento do HD e formação do código de segurança (códigos hash), a autoridade policial confessadamente rompeu o lacre e acessou diretamente o disco rígido, referindo, no entanto, que não alterou os arquivos. Segundo a sentença "houve alteração de arquivos na mídia apreendida. Essa alteração ocorreu após a apreensão, enquanto a mídia estava na guarda policial, pericial e judicial. (…) Todo esse contexto deixa claro que houve falhas na preservação do material apreendido. Aparentemente, os próprios arquivos que contêm os bancos de dados foram alterados, visto que são datados das 11h08 do dia apreensão, a qual teria ocorrido ao raiar do dia." Mesmo diante disso, a decisão foi pela licitude da prova e sua consequente manutenção nos autos, o que foi confirmado em grau recursal no TRF-4. (STJ, REsp nº 1435421/RS, 6ª Turma, Rel. Maria Thereza de Assis Moura).

5. ANÁLISE

5.1. Nunca usar evidência original para procedimentos

A evidência digital original deve ser mantida em segurança e devidamente documentada no formulário de cadeia de custódia, respeitando a sua integridade. Todo e qualquer procedimento a ser realizado para averiguação e análise da evidência, deve ser feito com uma cópia forense, ou a cópia da cópia forense. Desta maneira conseguimos preservar o material original, e trabalhar com as cópias para fins elucidativos.

5.2. Usar mídias de coleta totalmente limpos

É de suma importância que os dispositivos de armazenamento que irão receber a cópia forense da evidência, estejam "forensemente" limpos . Não devem contar um bit sequer que não devesse estar ali, caso contrário poderá contaminar a cópia da evidência e gerar um resultado inverídico.

5.3. Autenticidade da evidência

Para as provas digitais deve ser realizado o teste do hash, onde estará autenticando a cópia forense da evidência. Garantindo assim que a cópia que será usada para análise seja exatamente igual à evidência original.

A evidência deve estar disponível para ser consultada, quesitada ou examinada pelo assistente técnico de defesa, para garantir o direito da ampla defesa e do contraditório. (CPP, Art. 159o, parágrafo 6o).

6. MODELO

A cadeia de custódia deve seguir alguns padrões para a identificação e acompanhamento da evidência. Apresentaremos um modelo comumente usado e aceito para manter a cadeia de custódia.

6.1. Identificação do equipamento

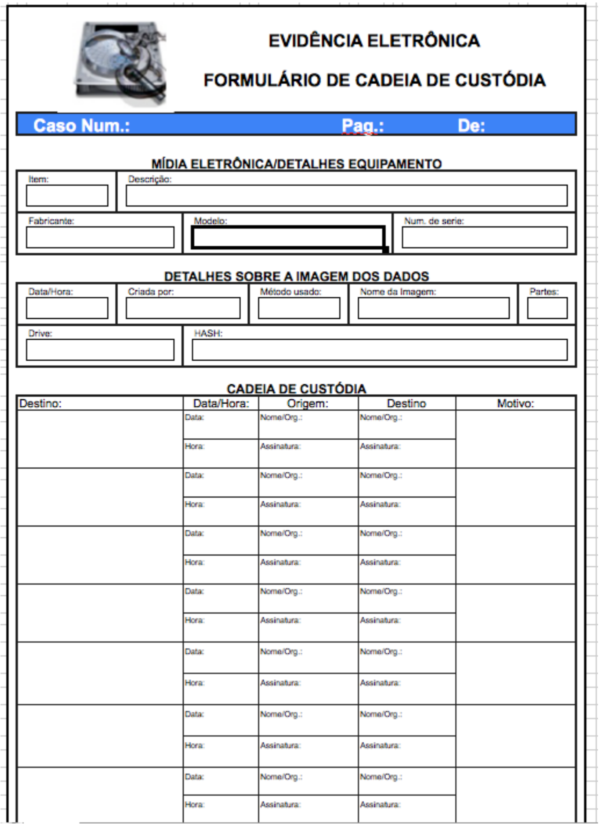
- Número do caso: deve estar contido o número do caso.
- Item: se coloca a numeração do item de acordo com o que foi catalogado.
- Descrição: identificação do equipamento, se pendrive, HDD, DVD, cartão de memória, smartphone, etc…
- Fabricante: quem fabricou o equipamento.
- Modelo: modelo específico do equipamento.
- Número de Série: número de identificação do equipamento junto ao fabricante.

6.2. Detalhes sobre a imagem de dados

- Data/hora: data e hora que a imagem foi finalizada.
- Criada por: perito que fez a imagem forense do equipamento.
- Método usado: método usado para copiar a imagem forense da mídia, podendo ser por softwares como Encase, FTK, dd, Caine, etc.
- Nome da imagem: nomenclatura dada a imagem criada a partir do equipamento.
- Partes: quantidade de partes que a imagem foi dividida.
- Drive: local de armazenamento da imagem forense (Ex.: HD externo, HDD, SDD, pendrive, etc.).
- Hash: identificação algorítmica da imagem, para que haja uma melhor aceitação deve constar o hash MD5 e SHA1 e/ou SHA256.

6.3. Cadeia de custódia

- Destino: local que a evidência vai seguir.
- Data/hora: data e hora que a evidência sairá do local atual.
- Origem: Local atual da evidência.
- Destino: nome do local e da pessoa responsável pela guarda da evidência e sua cadeia de custódia.
- Motivo: motivo pelo qual a evidência está mudando o seu local.



EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: Pag.: De:

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item: Descrição:

Fabricante: Modelo: Num. de serie:

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora: Criada por: Método usado: Nome da Imagem: Partes:

Drive: HASH:

CADEIA DE CUSTÓDIA

Destino:	Data/Hora:	Origem:	Destino	Motivo:
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	

Figura 2. Formulário de cadeia de custódia.

7. CÓDIGO DE PROCESSO PENAL

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;

Art. 159 § 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."

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 consequências dessas alterações na dinâmica dos fatos.

8. CONCLUSÕES

Resultante de tal explanação, podemos perceber a importância do documento da Cadeia de Custódia, para que possa apresentar de forma cronológica a rastreabilidade e integridade da mesma. Para que a mesma possa ser aceita sem questionamentos diante do processo. O documento de cadeia de custódia se baseia no Código de Processo Penal, e deve ser aceito em todos os casos quando não houver a quebra da cadeia de custódia e a sua ausência é penosa, pois pode garantir a ilicitude da evidência.

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus que tem me dado forças e orientado, a minha esposa que sempre esteve ao meu lado, ao Marcos Monteiro a quem tem me inspirado a seguir na área e a APECOF (Associação Nacional dos Peritos em Computação Forense) que me abriu portas e incentivou a seguir essa maravilhosa área.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] CADEIA. Dicionário online Michaelis, 26 jun. 2019. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/cadeia/. Acesso em 26 de jun. 2019.

[2] CUSTÓDIA. Dicionário online Michaelis, 26 jun. 2019. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/cust%C3%B3dia/ Acesso em 26 de jun. 2019.

[3] BRASÍLIA. RENÊ CARVALHO DE BRITO. . Procedimento operacional padrão: : perícia criminal. Ministério da Justiça: Secretaria Nacional de Segurança Pública, Brasília, p. 91-91, set. 2013. Disponível em: https://www.novo.justica.gov.br/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf/view. Acesso em: 28 jan. 2019.

[4] BRASIL. Código de Processo Penal. Diário Oficial da República Federativa do Brasil. Brasília, DF, 13 out. 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm Acesso em 26 jun. de 2019.

[5] FDTK. Cadeia de Custódia. Disponível em: http://fdtk.com.br/wiki/tiki-index.php?page=formulario Acesso em 26 jun. 2019

[6] INFOSEC. Computer Forensics: Chain Of Custody. Disponível em: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/#gref Acesso em 27 jun. 2019

[7] JUSBRASIL. Superior Tribunal de Justiça STJ - RECURSO ESPECIAL : REsp 1435421 RS 2014/0029779-8 - Rel. e Voto. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/202282396/recurso-especial-resp-1435421-rs-2014-0029779-8/relatorio-e-voto-202282414?ref=juris-tabs Acesso em 29 jun. 2019.