Cadeia de custódia

Data do post	@July 27, 2021 9:00 AM (GMT)
status	In Progress
Palavras-chave	Evidências
checkbox	☐

A norma ISO 27037 traz diretrizes para identificação, coleta, aquisição e preservação de evidência digital e outras definições importantes como a distinção entre o processo de coleta e aquisição, conforme demonstrado a seguir:

- **Coleta**: processo de recolha dos objetos e ou itens que possam conter potencial evidência digital.
- **Aquisição**: processo de criação de cópia de dados. Imagem ou espelhamento do conteúdo de dispositivos de armazenamento. Utilizada para gerar uma cópia digital da evidência, garantindo a preservação do dispositivo em análise no seu estado original
- **Dispositivo digital**: qualquer mídia ou equipamento eletrônico/telemático utilizado para armazenar ou processar dados digitais
- **Dados voláteis**: dados que são especialmente propensos a alteração e que podem ser facilmente modificados.

Um dos principais tópicos abordados pela norma, refere-se aos procedimentos a tomar no primeiro contato com uma evidência. Esse é o trabalho do First Responder, conforme detalhado a seguir.

First Responder

Aula 2.1 : First Responder

Coletando a evidência

O processo de coleta é a obtenção de objetos que possam conter potencial evidência digital. Trata-se efetivamente do recolhimento dos itens físicos, que serão posteriormente submetidos a análise em laboratório. Caberá ao First Responder avaliar e decidir o melhor procedimento, considerando sua capacitação para remover o dispositivo, além de outras variáveis como custo, tempo e preservação da evidência, ou optar pelo processo de aquisição dos dados.

Além da coleta dos dispositivos digitais, deverão ser recolhidos do local outros objetos, tendo em contra sempre os cuidados necessários para preservação das evidências. Toda abordagem deve ser documentada.

Caso o dispositivo seja encontrado ligado, independente da realização da coleta, sempre que possível recomenda-se a realização do procedimento de aquisição dos dados, sobretudo para preservação das informações voláteis

Aquisição

Segundo a ISO 27037, o processo de aquisição envolve gerar uma cópia digital da evidência, com a respectiva documentação dos métodos e procedimentos utilizados neste processo. Estes procedimentos devem ser usados por outro perito e gerar a menor alteração possível na evidência.

O procedimento de aquisição deve gerar uma cópia digital da evidência, certificada através do uso de funções de verificação, de modo tal que produza um mesmo hash que a evidência original. Quand esse processo de verificação não for realizado, o First Responder deverá documentar o método utilizado, justificar o fato e eventuais procedimentos escolhidos.

Live Aquisition: desligar ou não desligar

No inicio do processo de aquisição dos dados, é comum existir uma dúvida sobre manter ou não um dispositivo ligado. Isso porque desligá-lo pode significar a perda de dados voláteis ou até mesmo impossibilitar um acesso posterior, já que em uma nova inicialização, o dispositivo pode ser protegido por senha ou criptografia. Por outro lado, não desligar o equipamento pode implicar em permitir a exclusão ou modificação de algum dado, por meio de procedimento remoto ou programa/script local em andamento.

Encontrando o sistema ligado e com acesso ao sistema operacional, é importante o perito coletar, por exemplo:

- Data e hora do sistema.
- Conexões de rede.
- Portas abertas.
- Usuários logados.
- Processos, serviços ou aplicativos em execução.
- Tarefas agendadas.
- Arquivos abertos.
- Cookies e histórico navegação.
- Cache e outras informações do browser.
- Favoritos.
- Logs em geral.
- Wipe da memória RAM.

> 💡 **Conteúdo na área de transferências:**
> A simples, mas muitas vezes negligenciada, inspeção por exemplo, do histórico de comandos e conteúdo armazenado na área de transferência, pode revelar detalhes importantes sobre o recente uso do dispositivo, incluindo eventuais tentativas de ocultar provas.

Mesmo suspeitando-se de algum procedimento de wipe em execução, que não possa ser interrompido por outro meio, não se deve desligar o computador através dos procedimentos habituais. Isso porque o desligamento a partir de procedimentos comandados pelo sistema operacional, ocasiona a limpeza e remoção dos dados armazenados na área de swap do disco. O swap é uma área de memória disponível nos discos rígidos, utilizada como um recurso adicional do sistema para armazenar temporariamente, conteúdos que estariam guardados na RAM, mas que foram movidos para o HD em função da necessidade de espaço. Comportando-se como uma extensão da RAM no disco, esta área pode conter importantes informações sobre o estado atual da máquina, que se perdem com o desligamento tradicional.

Nesses casos, portanto, a recomendação é remover o cabo de força, o que ocasionaria a manutenção dos dados de swap no disco para posterior análise. Vale lembrar que o procedimento de remoção do cabo pode causar outros problemas, devendo, portanto, ser utilizado somente em situações extremas, quando por exemplo o perito suspeitar de criptografia, wipe ou exclusão de dados em andamento.

Exame da Evidência

Em nenhuma hipótese deve-se realizar a análise pericial diretamente sobre a evidência coletada.

No caso da forense digital, a recomendação é que se gere duas novas cópias do material que será examinado, mantendo uma integralmente preservada, armazenada em local seguro e protegido, e destinando a outra cópia ao exame.

Cadeia de Custódia

Documento que mantém um registro de todo histórico da evidência.

Segundo a ISO 27037, a cadeia de custódia compreende o registro documental de toda a cronologia de movimentação de um vestígio.

Este documento deve ser criado no momento seguinte a coleta ou aquisição da evidência e deverá conter todo o seu histórico de localização e manuseio, desde o momento em que foi obtido até o seu estado atual.

A cadeia de custódia deve ser criada no momento seguinte a coleta ou aquisição da evidência e deverá conter todo o seu histórico de localização e manuseio, desde o momento em que foi obtido até o seu estado atual.

> “O propósito de manter o registro de cadeia de custódia é manter a identificação do acesso e movimento da potencial evidência digital a qualquer tempo” - ISO 27037

Formulário da Cadeia de Custódia

Segundo a ISO 27037 o registro da cadeia de custódia deverá conter as seguintes informações:

- Identificador único da evidência;
- Quem acessou/verificou a evidência e o tempo e local em que ocorreu;
- Motivo de a evidência ter sido verificada (qual caso e propósito) e a autoridade relevante
- Quaisquer evidência alterações digital,com justificativa e responsável. Inevitáveis a da respectiva.

FORMULÁRIO DE CADEIA DE CUSTÓDIA

NÚMERO DO CASO	20090226					
DETALHES DA MÍDIA OU EQUIPAMENTO						
ITEM	DESCRIÇÃO					
1	HD DO NOTEBOOK COM 2 GB DE CAPACIDADE					
FABRICANTE	MODELO	NÚMERO DE SÉRIE				
SAMSUNG	SGM2GB	ABC123456				
SOBRE A IMAGEM DOS DADOS						
DATA	HORA	CRIADA POR	FERRAMENTA USADA			
26/2/2009	10:53	SÍLVIO DO MONTE	EnCASE VERSION 3			
TIPO DE CÓPIA	HASH					
DISCO COMPLETO	4e3d2d5e5427953d7eda6ddc6627bf6b					
CADEIA DE CUSTÓDIA						
CÓDIGO	ORIGEM	DATA	HORA	DESTINO	DATA	HORA
1	LOCAL DE APREENSÃO	26/2/2009	17:00	PERÍCIA	26/2/2009	17:30