

Uma Masterclass de Perícia Judicial



Estruturando o Caos Digital

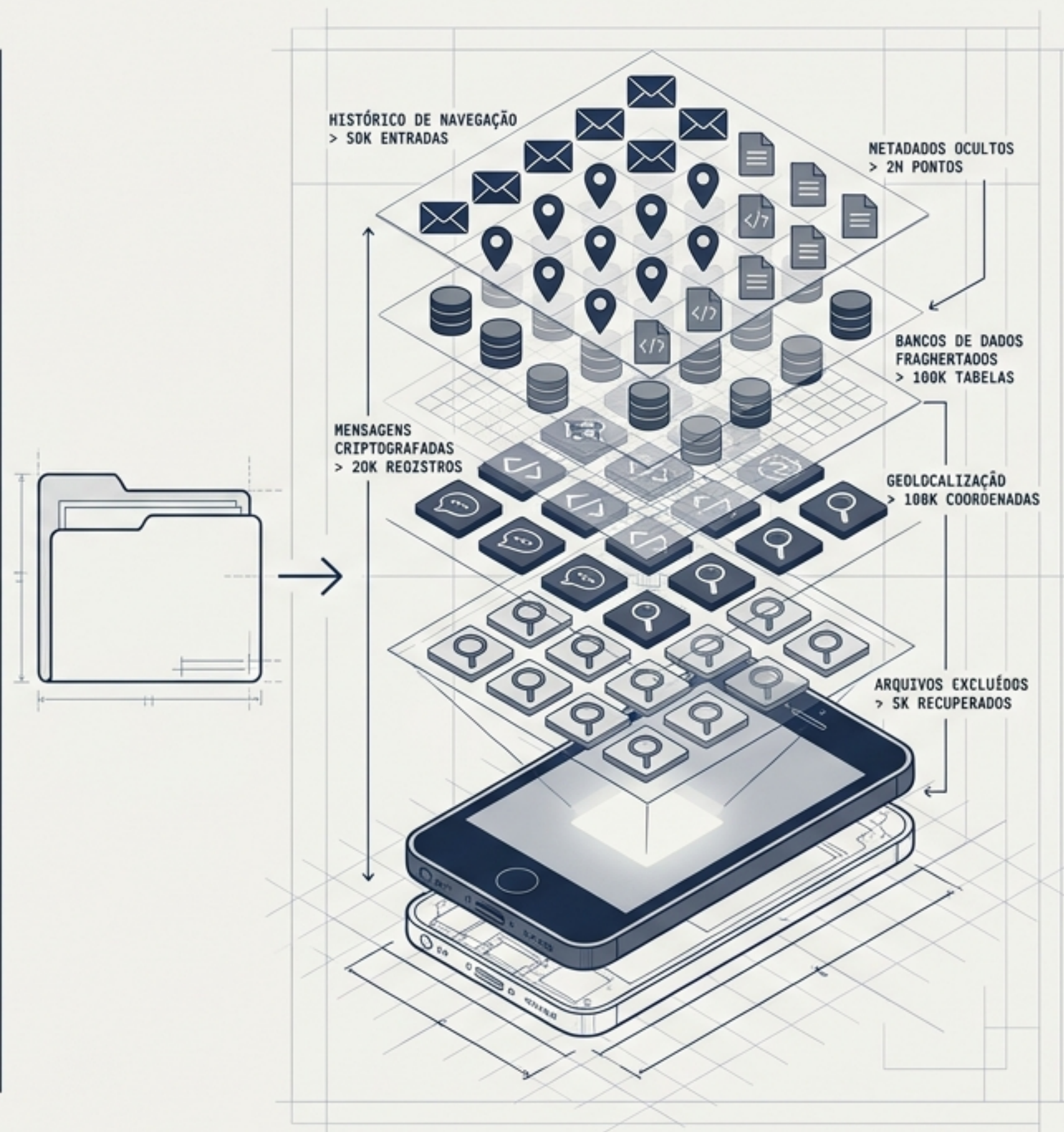
O Guia Definitivo para Indexação e Análise Forense
com Autopsy, IPED e Magnet AXIOM.

Por Perito Agenor Zapparoli

A Avalanche de Evidências Digitais

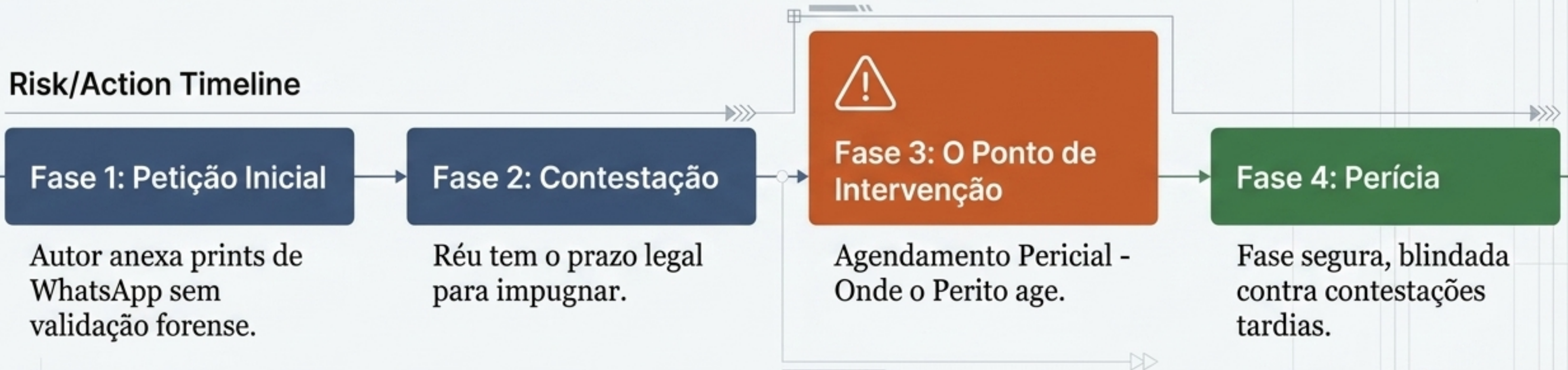
A digitalização transformou dispositivos em imensas fontes de provas. Um único celular moderno não contém apenas arquivos; ele abriga anos de histórico de navegação, metadados ocultos, bancos de dados fragmentados e mensagens criptografadas.

“ O Desafio da Volumetria: Realizar a análise manual de centenas de milhares de arquivos é humanamente inviável e tecnicamente arriscado.



A Armadilha da Preclusão Processual

Risk/Action Timeline



Adote uma postura preventiva logo no agendamento. Questione formalmente as partes sobre a veracidade das provas (como prints). Se o réu tentar impugnar tardiamente, o perito evidencia a preclusão, garantindo que o laudo não seja invalidado.

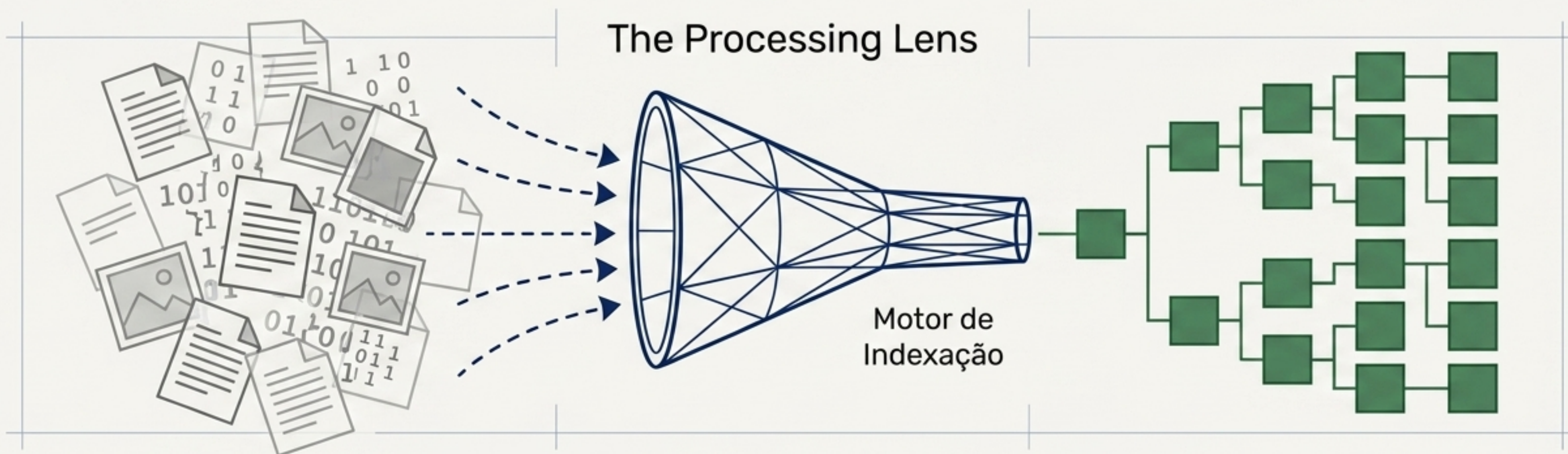
Zapparoli Golden Rule Callout

A Anatomia da Investigação Digital



O Motor de Indexação: Estruturando o Caos

Indexar não é simplesmente usar a barra de pesquisa do computador. É varrer terabytes de dados brutos e construir índices otimizados de texto, nomes e metadados.



Permite buscas instantâneas com suporte a expressões regulares (regex).



Alcança conteúdos dentro de arquivos compactados e registros excluídos.

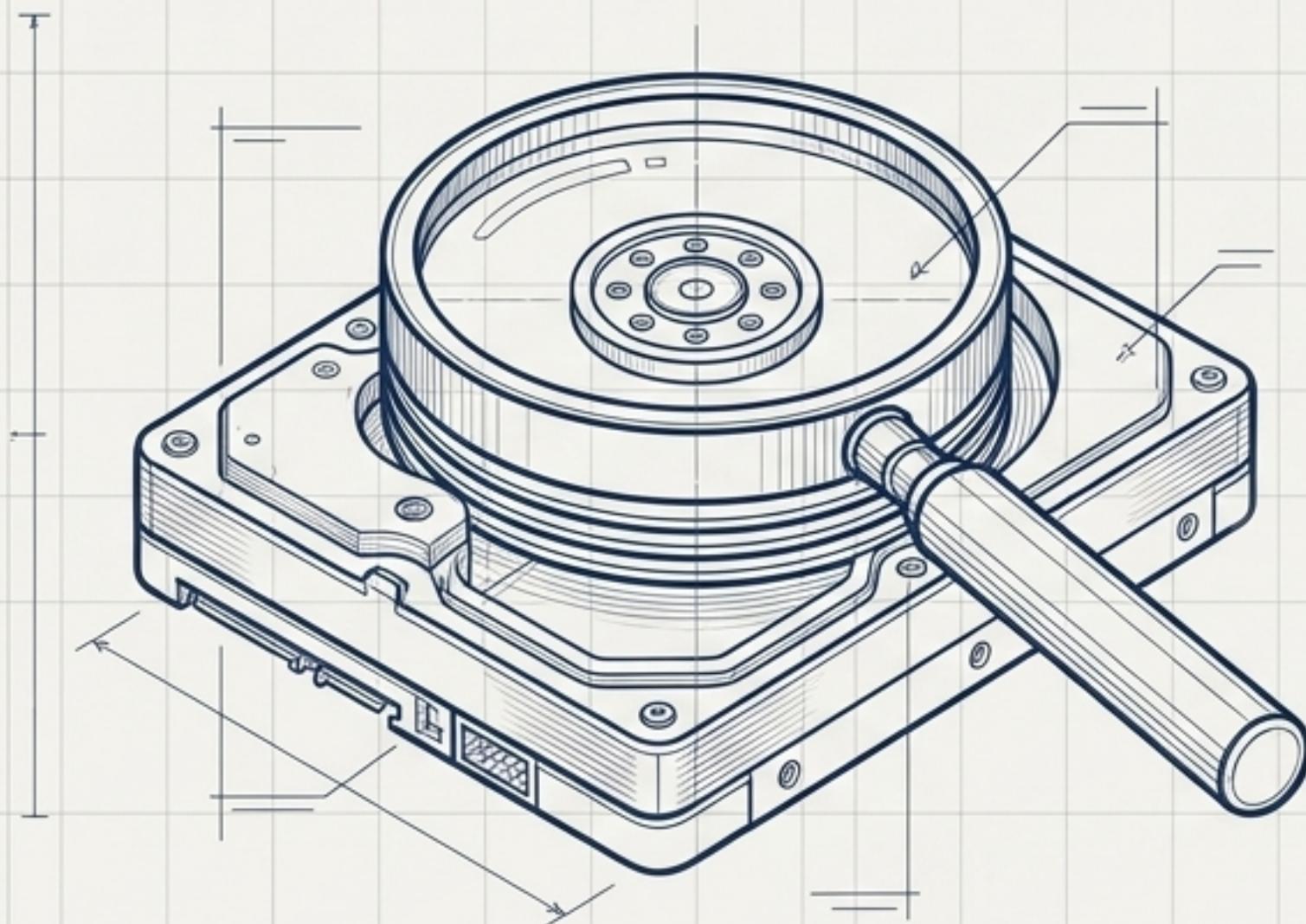


Transforma um emaranhado binário em informações visualmente correlacionadas.

Autopsy: A Fundação Open Source

Desenvolvido pela Sleuth Kit Labs (Liderança de Brian Carrier)

OPEN SOURCE



Tech-Spec

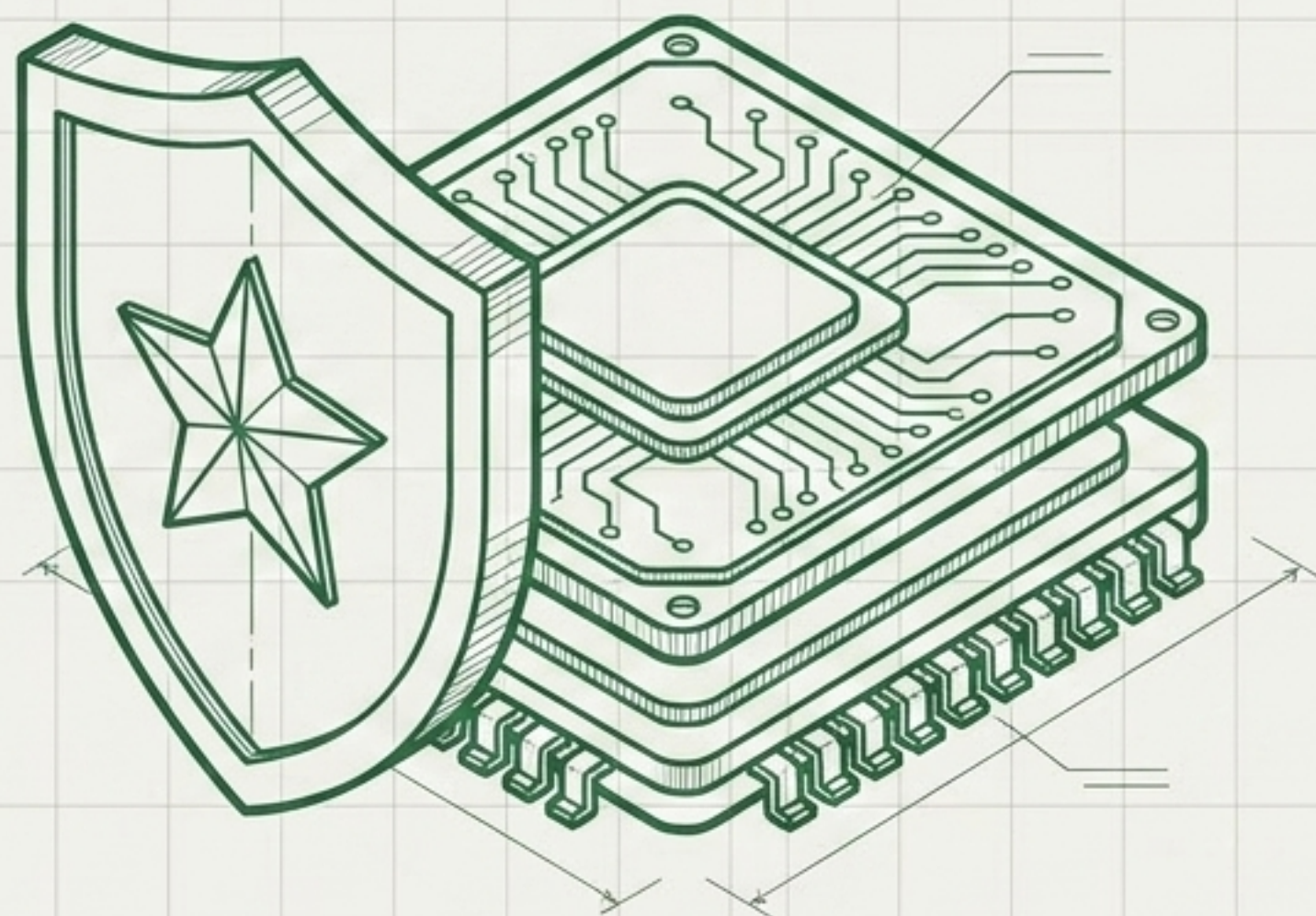
1	Licenciamento	Gratuito (Open Source).
2	Mecanismo	Interface gráfica construída sobre a biblioteca de linha de comando The Sleuth Kit.
3	Diferencial	Arquitetura altamente modular. Excelente para imagens de disco (RAW/DD, E01) e extrações lógicas.

“ Sendo gratuito, é ideal para profissionais independentes e pesquisadores, mas não se engane: possui robustez corporativa para recuperar arquivos e gerar linhas do tempo precisas.

IPED: A Força Bruta Nacional

Indexador e Processador de Evidências Digitais (Polícia Federal do Brasil)

CÓDIGO ABERTO



Tech-Spec

1	Licenciamento	Gratuito (GNU General Public License v3).
2	Mecanismo	Arquitetura hiper-otimizada para multithreading.
3	Diferencial	Projetado para dezenas de milhões de itens. Integra IA (reconhecimento facial, OCR) e parsers especializados para WhatsApp, Telegram e Skype.

“ A solução definitiva para volumetria extrema. O IPED resolve o gargalo de processamento de massas de dados gigantescas, sendo indispensável no contexto institucional brasileiro.

Magnet AXIOM: O Ecossistema Integrado

Solução Comercial de Última Geração (Magnet Forensics)

COMERCIAL /
ENTERPRISE



Tech-Spec

1	Licenciamento	Comercial/Pago (Nível Empresarial).
2	Mecanismo	Motores analíticos com IA para recuperação profunda e reconstrução de artefatos complexos.
3	Diferencial	Unificação de fontes. Reúne computadores, nuvem, mobile e IoT em um único caso. Mapeia conexões visuais automatizadas.

“ Quando o alvo usa simultaneamente um notebook, um smartphone e serviços em nuvem, o AXIOM brilha ao correlacionar essas evidências em uma visão única e unificada.

Matriz do Arsenal Forense

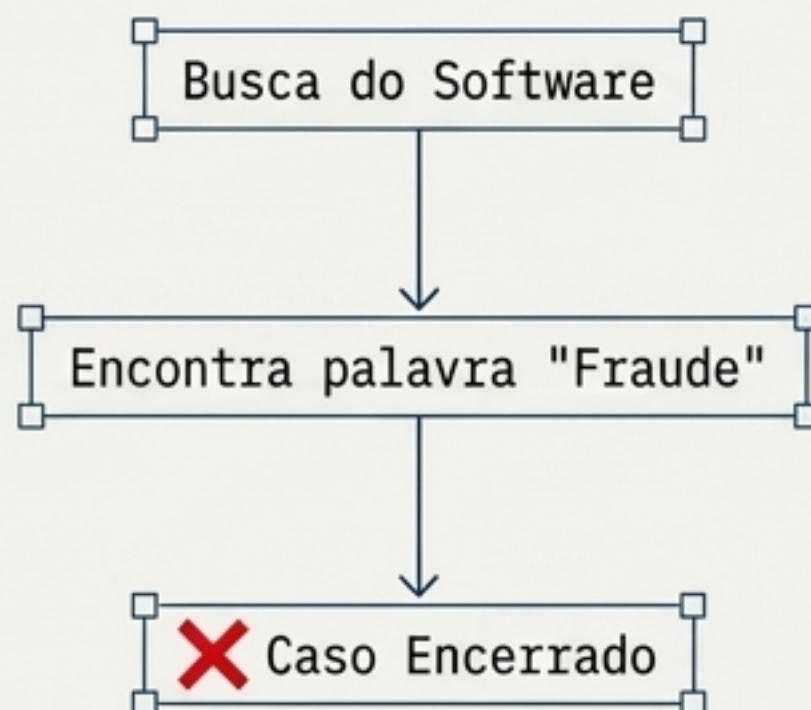
	Autopsy	IPED	Magnet AXIOM
Licenciamento	Gratuito/Open Source	Gratuito (GPLv3)	Comercial/Pago
Origem	Sleuth Kit Labs	Polícia Federal (Brasil)	Magnet Forensics
Superpoderes	Expansão Modular	Multithreading Extremo & OCR	Conexões Multi-Dispositivo & IA
Cenário Ideal	Análise clássica de disco e imagens E01.	Volumes massivos de dados nacionais e chats.	Investigações complexas cruzando mobile e nuvem.

O perito não deve ser dependente de uma única ferramenta. Escolha o software baseado no objeto da perícia, não apenas na popularidade.

A Ilusão da Conclusão Automática

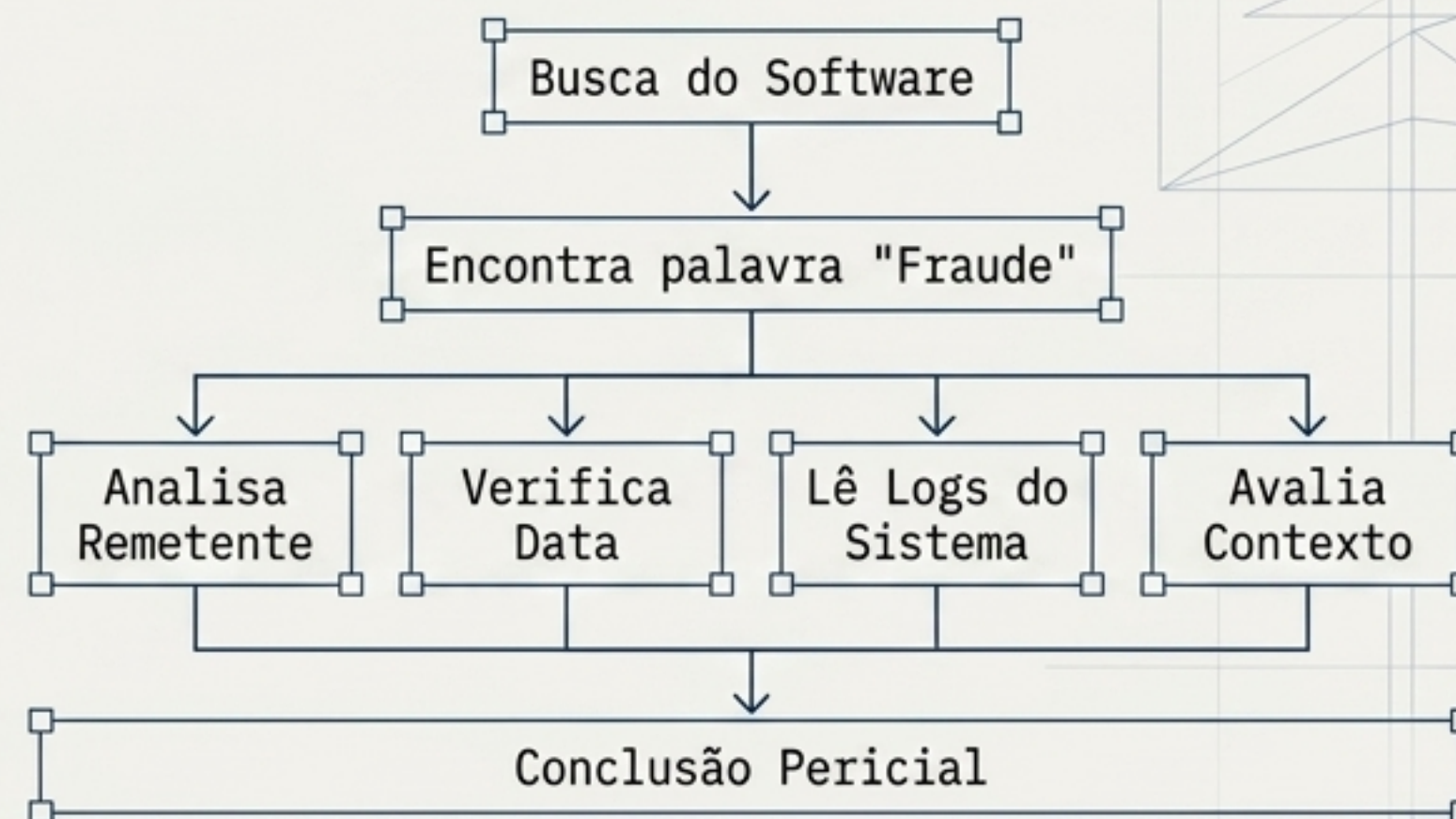
A Ilusão (O Erro do Iniciante)

Acreditar que a indexação "encontra a prova". A presença de um arquivo não prova autoria; ele pode ter sido criado pelo sistema, recebido ou baixado automaticamente.



A Realidade (O Raciocínio Pericial)

A indexação reduz o tempo de busca, mas não elimina a interpretação. O perito cruza a descoberta com metadados, contexto e linhas do tempo.



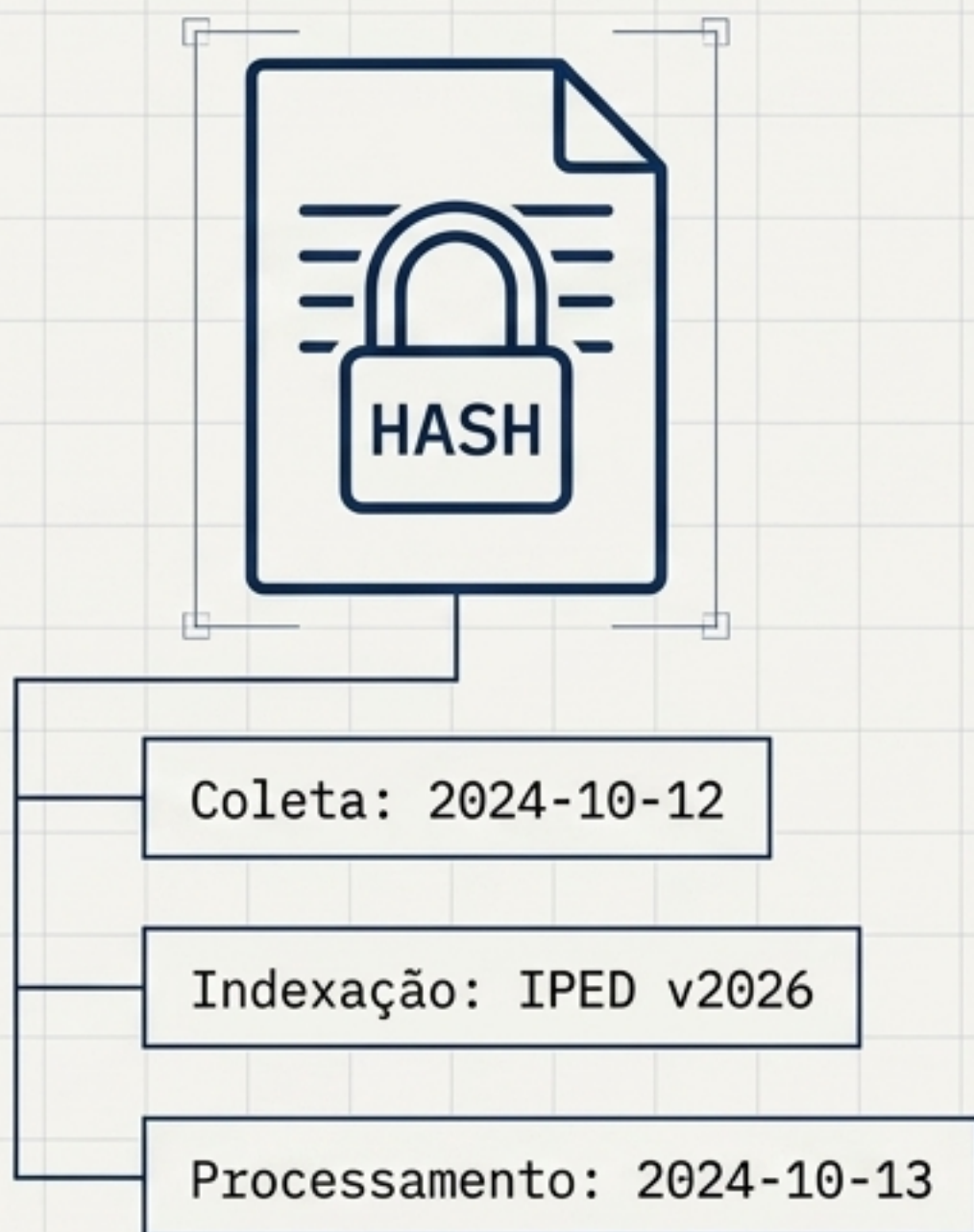
“

A existência de um arquivo não prova o crime. O software localiza a informação; o Perito interpreta o contexto.

”

Cadeia de Custódia e a Falsa Segurança

A utilização de ferramentas de indexação deve estar blindada por procedimentos estritos de preservação.



1. O Limite do Hash

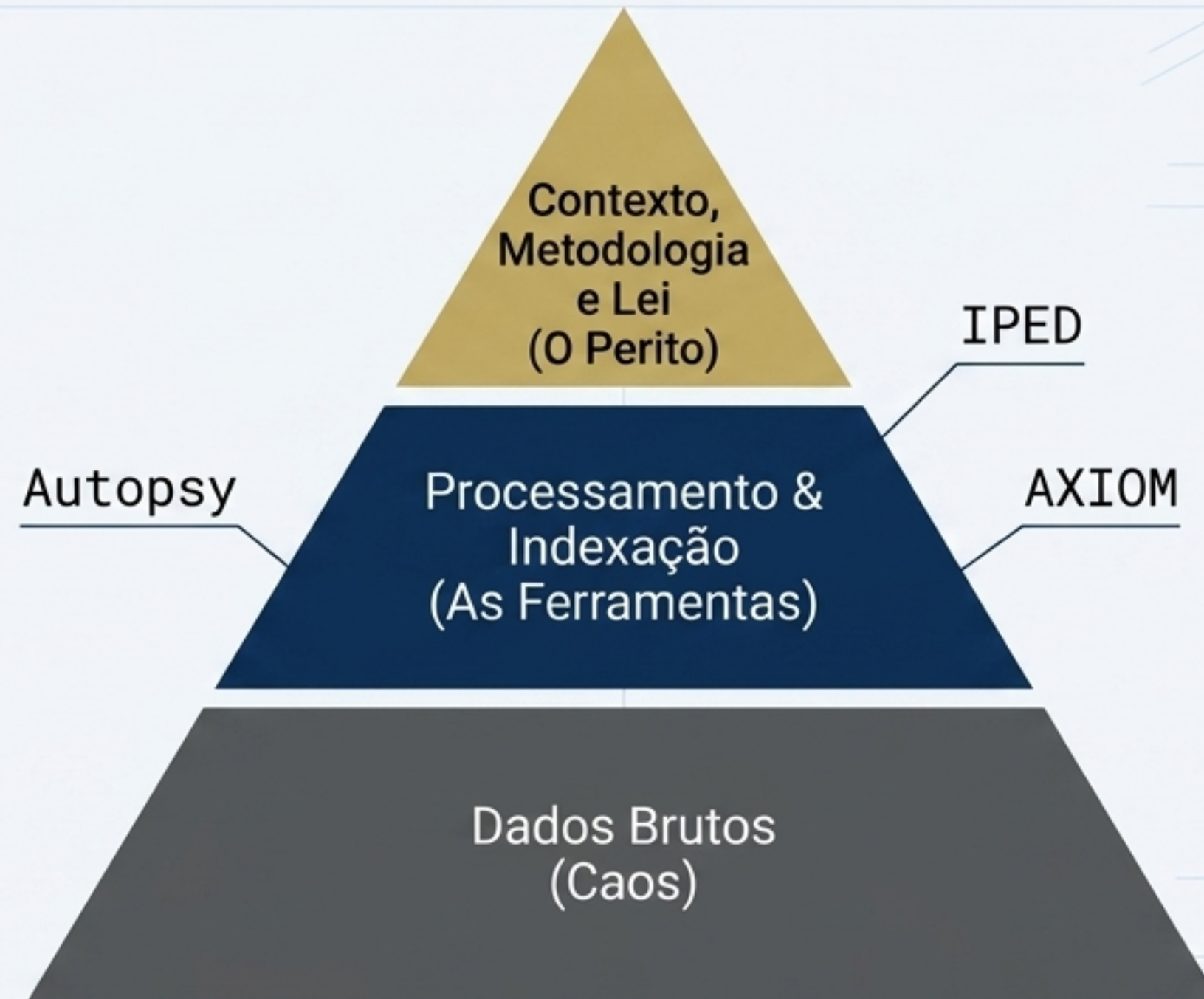
O código Hash garante que o arquivo não foi alterado após a coleta. Ele **NÃO** prova que o conteúdo original era verdadeiro ou obtido de forma legítima.

2. Reprodutibilidade Forense

O perito deve sempre registrar a versão exata do software utilizado. Atualizações futuras nos mecanismos de processamento podem gerar resultados divergentes ao tentar reproduzir o exame.

O Fator Humano

A Hierarquia da Verdade Forense



“A ferramenta é o microscópio da perícia digital: ela amplia a capacidade de observação do profissional, mas não substitui o conhecimento científico daquele que interpreta o que está sendo observado.”

Dominar a ferramenta é o básico. Dominar os fundamentos da computação forense e do rito processual é o que define o verdadeiro Perito Judicial.