

EMENTA — XXVIII CONGRESSO NACIONAL DE CRIMINALÍSTICA

Aos cuidados de: Comissão Científica do CNC 2026
Congresso Nacional de Criminalística

REF: Minicurso de Recuperação de Dados em Dispositivos de Armazenamento Danificados: HD, SSD e Dispositivos Móveis.

A presente ementa detalha o minicurso de caráter introdutório a ser ministrado no XXVIII Congresso Nacional de Criminalística (CNC 2026), voltado a peritos criminais e profissionais de inteligência. A proposta alia fundamentação técnica à apresentação de casos reais trabalhados em laboratório especializado no atendimento a forças de lei e polícias técnico-científicas, permitindo que o participante compreenda as possibilidades da perícia em dispositivos danificados e como extrair a maior quantidade de dados em cenários que parecem ser impossíveis de extrair informações. Durante o Minicurso as ferramentas da linha PC-3000 serão demonstradas como recurso avançado aliada ao laboratório de extração.

1. Objetivo

Apresentar, de forma acessível e aplicada, os fundamentos e as técnicas utilizadas na recuperação forense de dados em mídias danificadas. Discos rígidos (HD), unidades de estado sólido (SSD) e dispositivos móveis (smartphones). O curso visa capacitar os participantes a identificar o tipo e a extensão da falha, selecionar a abordagem de recuperação mais adequada e garantir a integridade probatória dos dados recuperados, com base em casos reais atendidos por um laboratório avançado.

2. Público-Alvo e Perfil da Turma

O minicurso é destinado a:

- Peritos criminais;
- Profissionais de inteligência;
- Analistas forenses;
- Policiais civis, policiais científicos e integrantes de instituições de segurança pública;
- Profissionais envolvidos em extração, preservação, recuperação ou análise de evidências digitais.

Nível: Introdutório. Não há exigência de conhecimento avançado em informática; é desejável familiaridade básica com sistemas operacionais Windows e conceitos de armazenamento de dados.

Vagas: Até 20 participantes .

3. Pré-requisitos e Infraestrutura Necessária

Por se tratar de um minicurso introdutório, não é obrigatório conhecimento avançado em eletrônica, recuperação de dados ou ferramentas especializadas. Recomenda-se familiaridade básica com informática, dispositivos de armazenamento e procedimentos de preservação de evidências digitais.

Notebook próprio com sistema operacional Windows 10/11, com pelo menos 8 GB de RAM e 50 GB de espaço livre em disco.

Softwares pré-instalados (instruções enviadas com antecedência pelo instrutor).

4. Conteúdo Programático (Ementa)

Horário	Atividade
08:00	Abertura — Introdução à Recuperação de Dados em Contexto Forense
08:30	Módulo 1 — Recuperação de dados em Discos Rígidos (HD)
09:20	Módulo 2 — Recuperação de dados em SSDs (Flash NAND)
10:10	Intervalo — Café e networking (15 min)
10:25	Módulo 3 — Recuperação de dados em Dispositivos Móveis (Smartphones)
11:20	Módulo 4 — Estudo de casos reais e elaboração de laudo pericial
12:00	Encerramento — Debate, dúvidas e considerações finais

Introdução à Recuperação de Dados em Contexto Forense (08:00 – 08:30 | 30 min)

- Diferença entre recuperação de dados convencional e recuperação aplicada à perícia criminal.
- Preservação da evidência digital, documentação técnica e cadeia de custódia.
- Riscos de ligar, inicializar, reparar ou manipular mídias danificadas sem diagnóstico prévio.
- Fluxo recomendado: recebimento, triagem, diagnóstico, extração.
- Casos reais de perda ou agravamento de evidências por procedimentos inadequados.
- Princípios fundamentais: integridade, cadeia de custódia e geração de hash
- Classificação das falhas em mídias de armazenamento: lógica, física, eletrônica e de firmware
- Ferramentas e ambiente de trabalho: Microscópio, câmera térmica, multímetro, estações de solda, imagens forenses e softwares livres.
- **Caso real introdutório:** HD e SSD apreendido em investigação criminal.

Módulo 1 — Recuperação em Discos Rígidos (HD) (08:30 – 09:20 | 50 min)

- Funcionamento básico de HDs: pratos, cabeças, motor, PCB, firmware e área de serviço.
- Setores defeituosos, falhas de cabeças, motor, danos por queda, impacto, oxidação e surtos elétricos.
- Falhas lógicas: MBR/GPT corrompido, tabela de partição perdida, sistema de arquivos danificado
- Técnica de clonagem setor a setor: uso de softwares especiais para lidar com instabilidades de leitura.
- Problemas de reconhecimento, instabilidade e falhas de firmware.
- Estratégias de leitura controlada, criação de imagem e recuperação parcial
- Recuperação de arquivos deletados: Conjunto de softwares para cada tipo de cenário e quando cada ferramenta é indicada
- **Caso real:** recuperação de dados sensíveis.

Módulo 2 — Recuperação em SSDs (09:20 – 10:10 | 50 min)

- Arquitetura flash NAND: diferenças entre SLC, MLC, TLC e QLC e implicações forenses
- NAND Flash, controladora, wear leveling, garbage collection e TRIM.
- O Problema de memórias flash, como dados são destruídos silenciosamente e o que ainda é possível recuperar com hardwares especiais

- Falhas comuns: dispositivo não reconhecido, degradação de células NAND, firmware corrompido e falha de controladora.
- Ferramentas: PC-3000 Portable PRO
- **Caso real:** SSD de notebook apreendido / leitura em baixo nível.

Módulo 3 — Recuperação em Dispositivos Móveis / Smartphones (10:25 – 11:20 | 55 min)

- Cenários comuns: aparelho sem tela, sem bateria, USB danificado, placa oxidada, aparelho molhado, queimado, em bootloop e destruição intencional.
- Memória interna: chips eMMC e UFS
- Diferença entre extração lógica, sistema de arquivos e extração física.
- Ferramentas utilizadas em laboratórios de forças de lei
- Conceitos introdutórios de reparo mínimo para extração, Test Point, modos de processadores, vulnerabilidades, ISP, chip-off e transplante de componentes.
- **Caso real do laboratório:** smartphone destruído na busca e apreensão.

Módulo 4 — Estudo de Casos Reais e Laudo Pericial (11:20 – 12:00 | 40 min)

- Análise comparada de três casos reais anonimizados atendidos pelo laboratório do instrutor
- Estudos de Casos Reais, Relatórios Técnicos e Subsídios para Laudo Pericial.
- Como explicar limitações técnicas e inviabilidade de recuperação.
- Erros comuns que podem inviabilizar a recuperação.
- Discussão aberta, perguntas e encerramento.

5. Metodologia

O minicurso será conduzido em formato teórico-demonstrativo, com abordagem introdutória e aplicada à realidade da perícia criminal e da inteligência policial. Serão utilizados casos reais atendidos em laboratório especializado em recuperação de dados e suporte a forças de lei, incluindo situações envolvendo dispositivos oriundos de polícias técnico-científicas.

A dinâmica incluirá apresentação técnica, demonstrações em software, discussão de cenários reais, análise de limitações técnicas e orientação sobre boas práticas para preservação, recuperação e encaminhamento de mídias danificadas.

Wellington Rodrigues

Especialista em recuperação de dados e perícia digital, com atuação em casos complexos envolvendo HDs, SSDs, celulares e dispositivos de armazenamento danificados. Atua no suporte técnico a instituições de segurança pública, polícias técnico-científicas, ministérios públicos e laboratórios forenses, com experiência em recuperação de dados em cenários críticos, extração de evidências digitais e treinamento técnico especializado.

Legacy Lab

tom@legacy.tec.br | 11 940593753

Barueri, São Paulo, 08 de junho de 2026