Laudo Nº {NUMERO} – {UNIDADE}

LAUDO DE PERÍCIA

(INFORMÁTICA)

Em {DATA\_HOJE}, no XXXXXXXXXXXX da XXXXXX no Estado do XXXXX, designado pela XXXXX, XXXXX XXXXXXXXXXXXXX, o Perito {PERITO1} elaborou o presente laudo pericial, no interesse do(a) {NUMERO\_IPL}, a fim de atender à solicitação do(a) {AUTORIDADE\_FUNCAO} {AUTORIDADE\_NOME}, contida no(a) {DOCUMENTO} de {DATA\_DOCUMENTO}, e registrado(a) no Sistema de Criminalística sob o nº {NUMERO\_CRIMINALISTICA} em {DATA\_CRIMINALISTICA}, descrevendo com verdade e com todas as circunstâncias tudo quanto possa interessar à Justiça e respondendo aos quesitos formulados, abaixo transcritos:

“Pedido de exame...”

1. MATERIAL

O presente laudo refere-se ao exame dos seguintes materiais:

1. OBJETIVO

Os exames têm por objetivo extrair e processar o conteúdo do material descrito na seção anterior, atendendo à solicitação contida no expediente supracitado.

1. EXAME

III.1 - Identificação, extração e processamento

Inicialmente foram realizados o levantamento e a identificação do material enviado para exame, cujos resultados encontram-se na seção I.

Em seguida, por meio de técnicas forenses apropriadas, o material original foi copiado para arquivos de imagem de disco em outra mídia de armazenamento. Como medida de segurança, os processamentos seguintes foram realizados sobre a cópia, preservando-se o original.

Por meio do programa Indexador e Processador de Evidências Digitais – IPED v4.1.0, procedeu-se a extração forense de conteúdo do material examinado. Cabe salientar que este processo atinge não apenas os arquivos diretamente acessíveis, mas também aqueles previamente apagados que puderam ser recuperados.

Demais configurações utilizadas no processamento encontram-se dentro do diretório “*indexador*”, incluindo, entre outras, o arquivo “*marcadores.iped*” contendo os marcadores salvos por este signatário.

Logo após a geração do conteúdo para análise, foram realizadas buscas automáticas, executadas pela ferramenta IPED, por assinaturas digitais de arquivos (“*hashes*”) associados à pornografia infanto-juvenil. Além disso, também foram realizadas pesquisas, utilizando filtros disponíveis na ferramenta e inspeção visual direta do conteúdo dos arquivos para procurar outros arquivos com conteúdo relacionado à pornografia infanto-juvenil bem como para remover possíveis falsos positivos provenientes das categorizações automáticas. Ressalta-se que, por conta do volume de dados e complexidade da tarefa, esta técnica não é exaustiva.

Ademais, foram realizadas buscas por programas de compartilhamento, que possibilitem indicar arquivos que tenham sido compartilhadas na internet.

III.2 – Identificação do Sistema Operacional e Usuário

Identificou-se, em condição ativa, os seguintes sistemas operacionais:

1. Sistemas operacionais ativos no(s) material(is) examinado(s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sistema Operacional** | **Usuário de Registro** | **Nome do Computador** | **Data de Instalação (UTC)** | **Data do Último Desligamento (UTC)** |
| xxx | xxx | xxx | xxx | xxx |

O(s) seguinte(s) usuário(s) estava(m) configurado(s) para acesso à instalação do Windows encontrada:

1. Usuário(s) configurado(s) no(s) sistema(s) operacional(is)

|  |  |  |
| --- | --- | --- |
| **Nome do Usuário** | **Data/hora do último login (UTC)** | **Quantidade de logins efetuados** |
| xxx | xxx | xxx |

III.3 – Vídeos de Pornografia Infantil

No material examinado foram identificados XX (xx) arquivos de vídeos com indícios de cenas de sexo explícito ou pornográficas, envolvendo indivíduos com aparência de criança ou adolescente. Os vídeos totalizavam XX e estavam armazenados, majoritariamente, nas pastas XX. Destes arquivos, XX se encontravam ativos no sistema

Os vídeos foram extraídos e gravados no relatório presente na mídia óptica anexa ao laudo, na categoria “*Provavelmente* *vídeos contendo PI*”, acompanhados de imagens com cenas extraídas dos referidos vídeos como forma alterativa de visualização.

As Figuras XX a seguir mostram imagens de cenas de XX (xx) dos referidos arquivos, incluídas como exemplo do teor dos vídeos encontrados no material examinado.

Figura 1 – XXX

Figura 2 – XXX

III.4 – Imagens de Pornografia Infantil

No material examinado foram identificados XX (xx) arquivos de imagens com indícios de cenas de sexo explícito ou pornográficas, envolvendo indivíduos com aparência de criança ou adolescente. As imagens totalizavam XX e estavam armazenados, majoritariamente, nas pastas XX. Destes arquivos, XX se encontravam ativos no sistema

As imagens foram extraídas e gravadas no relatório presente na mídia óptica anexa ao laudo, na categoria “*Provavelmente* *imagens contendo PI*”.

As Figuras XX a seguir mostram imagens dos referidos arquivos, incluídas como exemplo do teor das imagens encontradas no material examinado.

Figura 3 – XXX

Figura 4 – XXX

III.5 – Compartilhamento de Pornografia Infantil

XXX

III.6 – Garantia de Integridade

Para possibilitar uma posterior verificação da integridade e autenticidade dos dados, foram calculados os códigos de integridade – função unidirecional de resumo criptográfico (hash) utilizando o algoritmo Secure Hash Algorithm 256 (SHA-256) – de todos os arquivos gerados. O resultado foi armazenado no arquivo “hashes.txt”, localizado na raiz da mídia em anexo. Por sua vez, o arquivo “hashes.txt” passou pelo mesmo processo, cujo resultado encontra-se a seguir:

1. *Hash* SHA -256 do arquivo “hashes.txt”.

|  |
| --- |
| XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |

Dessa forma, qualquer alteração do conteúdo (remoção, acréscimo, alteração de arquivos ou parte de arquivos), bem como sua substituição por outro com teor diferente, pode ser detectada.

III.7 – Disponibilização

Como resultado do processamento, os arquivos de interesse extraídos do material questionado são armazenados na pasta “Exportados” e, juntamente da ferramenta gráfica para análise “IPED-SearchApp.exe”, foram copiados para mídia anexa. Esta ferramenta permite o acesso aos dados por meio de interface gráfica, incluindo diversas funcionalidades de análise, tais como filtragem por categoria, busca indexada e pré-visualização do conteúdo. Deve-se utilizar um computador com Windows e Java 64 bits atualizados para um bom funcionamento do aplicativo de análise. Como forma alternativa de análise, também se encontra no diretório o arquivo “relatório.htm” para visualização dos dados extraídos, também já categorizados, em um navegador de internet.

A pasta contendo todos os arquivos encontra-se compactada em um arquivo “.7z”. Para extrair seu conteúdo, indica-se abrir o arquivo com o programa “7zip” e comandar sua extração. Nos casos em que o volume de dados não caiba em uma única mídia anexa, os arquivos/pastas são compactados em arquivos de formato “7z” de múltiplas partes, gerando arquivos com as extensões “.7z.001”, “.7z.002” e assim sucessivamente. Cada arquivo desses é copiado para uma das mídias anexas. Para acesso à pasta com o conteúdo extraído, indica-se copiar os arquivos de todas as mídias anexas para uma mesma pasta local e abrir o primeiro arquivo com um programa de descompactação, como o “7zip”, comandando a sua extração (o programa reconhecerá automaticamente os demais arquivos).

Foi produzido uma cópia do conteúdo em anexo que permanecerá arquivada neste Núcleo de Criminalística, juntamente com uma cópia deste Laudo

1. RESPOSTAS AOS QUESITOS

XXX

1. CONCLUSÃO

O material encaminhado a exame para disponibilização dos dados dos usuários nele contido, conforme a requisição e objetivos apresentados na seção II, passou pelas seguintes etapas:

1. Identificação do material
2. Cópia forense do material questionado;
3. Processamento do material utilizando a ferramenta IPED, versão 4.1.0.;
4. Análise dos arquivos processados para resposta aos quesitos.
5. Garantia de integridade dos arquivos através da geração do arquivo “hashes.txt”, cujo *hash* SHA-256 foi apresentado na Tabela 3 – da seção III ;
6. Disponibilização do material para análise em mídia anexa.

Tendo por bem esclarecido o assunto, o Perito devolve com o Laudo todo material descrito na seção I, em embalagens plásticas com os códigos de lacre a seguir:

1. Registros internos dos materiais devolvidos

|  |  |
| --- | --- |
| **Registro Interno do material** | **Código de Lacre** |

Nada mais havendo a lavrar, o Perito encerra o presente Laudo, produzido em XX páginas numeradas e XX mídia(s) óptica(s) em anexo, que lido e achado conforme, segue assinado.

1. ANEXO

XXXXX

Registro Interno do Material: XXXX

Código do Lacre: XXX

(assinado digitalmente)

**{PERITO1}**

**Perito**