SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
SERVIÇO DE PERÍCIAS EM INFORMÁTICA - SEPINF/DPDCE/INC/DITEC/PF

ANEXO I – ESPECIFICAÇÃO TÉCNICA

1. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

1.1. Deve ser fornecido, na forma de subscrição e pelo período de 36 (trinta e seis) meses, ferramenta pericial para análise de computadores e aparelhos celulares (Magnet Axiom Advanced - Licenciamento Dongle) com licença de uso na modalidade Subscrição, garantia, atualização e suporte técnico inclusos, que atenda aos seguintes requisitos mínimos.

1.1.1. Possuir suporte à decodificação de dados de dispositivos móveis, HDD, SSD, dispositivos USB e pastas de arquivos;

1.1.2. Permitir a decodificação de dados de dispositivos móveis com sistema operacional Android, e iOS;

1.1.3. Permitir a decodificação de dados de sistemas operacionais Windows, macOS, Linux;

1.1.4. Gerar relatórios nos formatos XML, HTML, CSV ou XLS, PDF e em formato portátil;

1.1.5. Permitir o cálculo de HASH MD5 e SHA-256;

1.1.6. Permitir realizar pesquisas utilizando textos, keyword, REGEX e GREP;

1.1.7. Permitir realizar a decodificação e análise dos dados utilizando uma única plataforma;

1.1.8. Permitir aplicação de filtros para auxiliar a pesquisa por artefatos;

1.1.9. Permitir realizar a marcação de arquivos por meio de tags;

1.1.10. Permitir gerar visualização utilizando Timeline;

1.1.11. Permitir visualizar dados que possuem dados geográficos no mapa (geolocalização);

1.1.12. Permitir realizar uma pré-visualização dos arquivos analisados em uma mesma interface;

1.1.13. Permitir visualizar os arquivos no formato Hexadecimal para uma análise mais detalhada dos dados;

1.1.14. Permitir a exportação dos dados encontrados no arquivo de evidência;

1.1.15. Permitir a recuperação de arquivos deletados e não sobrescritos;

1.1.16. Permitir colaboração e compartilhamento de evidências;

1.1.17. Permitir recuperar o Backups do iTunes;

1.1.18. Permitir recuperar informações quando um arquivo de torrent foi criado, modificado e baixado;

1.1.19. Permitir busca por palavra-chave em sistema de arquivos;

1.1.20. Permitir analisar artefatos P2P em dispositivos Android;

1.1.21. Permitir verificação baseada em Hash de imagem forense E01;

1.1.22. Possuir interface em no mínimo Inglês ou Português – Brasileiro;

1.1.23. Permitir a inserção da chave de criptografia de um disco criptografado com BitLocker antes do processamento do mesmo;

1.1.24. Permitir a criação de perfis de artefatos para diferentes tipos de casos;

1.1.25. Possuir a capacidade de realizar o correlacionamento dos dados;
1.1.26. Possuir funcionalidade de Inteligência Artificial para auxiliar na identificação de evidências, com suporte para interações em linguagem natural através de assistente virtual (chat);
1.1.27. Suporte a Imagens forenses de evidências no mínimo com os seguintes formatos de arquivo: E01, Ex01, L01, Lx01, AD1, dd, raw, bin, img, dmg, vmdk, vhd, vdi, xva, ufd, ufdx, zip, tar;
1.1.28. Suporte para decodificação e análise de dados extraídos com as ferramentas forenses Cellebrite Inseyts e Magnet GrayKey;
1.1.29. Suporte aos sistemas de arquivos: NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2, APFS;
1.1.30. Detecção automática de criptografia Truecrypt, Bitlocker, PGP, e Safeboot;
1.1.31. Capacidade de pré-visualização de arquivos plist;
1.1.32. Capacidade de pesquisa do espaço não alocado em uma imagem APFS;
1.1.33. Suporte de análise para itens recuperados de $RECYCLE.BIN;
1.1.34. Permitir a decodificação e análise da dados capturados de memória RAM;
1.1.35. Permitir a comparação de hashes com bases especializadas, como Project VIC;
1.1.36. Capacidade de análise de retorno de mandados judiciais de dados provenientes de nuvens, considerando ao menos Instagram, Facebook, Snapchat, Twitter, Google e Apple;
1.1.37. Uso de tokens extraídos da memória de aparelho celular para acesso a serviços e cópia forense de dados de serviços com armazenamento de dados na nuvem, contornando o segundo fator de autenticação, se necessário;
1.1.38. Localização e extração de tokens do computador (Windows, macOS);
1.1.39. Reconstrução de páginas WEB;
1.1.40. Recuperação de dados públicos de redes sociais;
1.1.41. Suporte fontes com duplo fator de autenticação;
1.1.42. Permitir agregar várias fontes de dados em um único caso;
1.1.43. Permiti detectar automaticamente possíveis imagens de conteúdo ilícito, como abuso infantil, substâncias proscritas e armas;
1.1.44. Permitir a identificação de carteiras, chaves privadas e análise de transações em blockchain, auxiliando em investigações envolvendo criptomoedas;
1.1.45. Visualização de SQLite;
1.1.46. Visualização em formato Hexadecimal;
1.1.47. Visualização de geolocalização em mapas;
1.1.48. Definir e alterar fuso horário padrão;
1.1.49. Customização de relatórios;
1.1.50. Recuperação de imagens, localizações, strings e demais arquivos apagados (carving);
1.1.51. Tratamento de banco de dados de aplicativos não categorizados, através do banco de dados (Assistente do SQLite);

1.1.52. Geração de dicionário de palavras e números, para ser utilizado como referência de ataque para quebra de senha;
1.1.53. Customização e execução de scripts Python;
1.1.54. Permitir atualização e suporte técnico por 36 meses;
1.1.55. Fornecer Suporte técnico (8X5);
1.1.56. Compatibilidade com a arquitetura tecnológica dos laboratórios forenses de informática, com Workstations baseadas prioritariamente em Sistemas Operacionais Windows