Estudo Técnico Preliminar

1. Informações Básicas

Número do processo: 00190.105003/2020-09

2. Descrição da necessidade

O presente documento trata da necessidade de aquisição de **solução forense para extração de dados e análise de equipamentos eletrônicos portáteis, tais como celulares, *pen drive*s**. Inúmeros trabalhos realizados na CGU, tais como produção de informações de inteligência, processo administrativo disciplinar (PAD) e operações especiais, necessitam analisar informações provenientes de equipamentos eletrônicos: estações de trabalhos, discos rígidos, celulares, entre outros. Atualmente, a infraestrutura de forense da DIE não dispõem de ferramentas para extração e análise de equipamentos portáteis, em especial os telefones celulares e smartphones. Desse modo, essa contratação tem por objetivo suprir essa necessidade.

3. Área requisitante

Área Requisitante	Responsável
Diretoria de Pesquisas e Informações Estratégicas - DIE	André Luiz Monteiro da Rocha

4. Necessidades de Negócio

Solução forense para extração de dados e análise de equipamentos eletrônicos portáteis;

Extração, análise e desbloqueio dos principais dispositivos móveis comercializados no país, incluído os equipados com os chipsets Qualcomm, Exynos, Spreadtrum e MTK, e dos principais sistemas operacionais para smartphones;

Solução para extração e análise de dados a partir de serviços de computação em nuvem (Cloud);

Análise de múltiplos dispositivos com objetivo de identificar vínculos entre seus usuários;

Treinamento nas soluções de extração e análise de dados;

Direito de atualização e suporte técnico pelo prazo de pelo menos 60 (sessenta) meses;

Suporte técnico (8X5).

5. Necessidades Tecnológicas

Requisitos de software forense para acesso a dados de dispositivos móveis e sistemas computacionais em nuvem (Cloud), para demandas em laboratório e em campo:

Funcionalidade
Funcionalidades de Desbloqueio e Extração (Física e Lógica) de Dispositivos Móveis
Extração seletiva
Extração lógica de Ios
Extração física de Ios
Extração lógica de Android
Extração através do modo EDL com descriptografia
Extração de celulares com descriptografia de chipsets MTK
Extração do tipo Smart ADB
Extração de dispositivos Samsung Qualcomm com descriptografia
Desbloqueio Android Genérico
Downgrade de APK
Extração de Huawei Kirin
Extração de LG LAF
Extração Samsung ADB
Extração através do modo TWRP
Extração de celulares com chipsets CoolSand

Extração de celulares com chipsets Spreadtrum
Extração parcial de iPhone bloqueado via checkm8
Extração completa de iPhone desbloqueado via checkm8
<u>Funcionalidades de Decodificação e Análise de Dispositivos Móveis</u>
Emulação de Android
Enriquecimento de geolocalização
Recuperação de dados públicos de redes sociais
Identificação de aplicativos não suportados
Detecção de Malware
Decodificação JTAG
Customização e execução de scripts Python
Visualização de SQLite
Visualização de Plist
Visualização em formato Hexadecimal
Visualização em linha de tempo
Visualização de geolocalização em mapas
Suporte a conjuntos de Hash
Customização de relatórios
Filtro avançado

Lista de palavras-chave
Enriquecimento dos identificadores de BSSID de forma online ou offline para trazer endereços de redes Wireless
Tradução automática de informações de geolocalização (latitude e longitude) em endereços
Captura e gravação de telas da solução durante o processo de investigação como documentação adicional visando a complementação do relatório final
Busca por padrões de informações em bancos de dados para criação automática de parser das soluções não suportadas
Recuperação de imagens, localizações, strings e demais arquivos apagados (carving)
Descoberta de dados de forma aprimorada por meio de técnica de Heurística (AppGenie)
Tratamento de banco de dados de aplicativs não categorizados, através do banco de dados (Assistente do SQLite);
Geração de dicionário de palavras e números, para ser utilizado como referência de ataque para quebra de senha
Suporte a evidências encaminhadas através de ordem judicial por fabricantes, tais como: Apple, Instagram, Facebook, Google, Snapchat, Discord, TextNow, SkyECC
Classificação de imagem e vídeo por categorias (ex: dinheiro, placas de veículos, cartão de crédito, quartos de hotel, faturas, documentos manuscritos, documentos)
Identificação de arquivos por meio de algoritmo de HASH, incluindo suporte a banco de dados do Projeto VIC e CAID
Detecção de transações através de criptomoedas, incluindo o endereço e os dados do dispositivo
Recuperação de dados de arquivos no formato TAR sem a necessidade de descompactação
<u>Funcionalidades de Extração e Análise de Dados de Serviços Computacionais em Nuvem</u>
Recuperação de rotas TCP/IP

Recuperação de páginas WEB
Configuração de Proxy
Recuperação de dados públicos de redes sociais
Localização e extração de tokens do computador (Windows e macOS)
Localização e extração de tokens do celular
Suporte fontes com duplo fator de autenticação
Extração não rastreável pelo usuário
Captura e/ou gravação de telas

Solução para extração e análise de dados a partir de plataformas eletrônicas portáteis, tais como smartphones, tablets, cartões de memória, cartões SIM, drones etc. A solução deve vir acompanhada de todos os cabos, conectores e acessórios necessários para extração e análise de todas as plataformas eletrônicas portáteis suportadas;

Extrair e analisar dados dos principais aparelhos móveis disponíveis no mercado brasileiro, incluindo, no mínimo, as seguintes marcas: Acer, Apple, Asus, BlackBerry, Huawei, LG, Lenovo, Microsoft, Motorola, Nokia, Samsung, Sony e Xiaomi;

Extrair e analisar dados dos principais sistemas operacionais para aparelhos móveis, contemplando, no mínimo: iOS, Android, BlackBerry, Symbian e Windows Phone;

Permitir, para fim de extração e análise de dados, o desbloqueio dos dispositivos que utilizam senha de padrão geométrico, de número PIN ou de reconhecimento facial, para a grande maioria dos modelos de celulares e de smartphones comercializados no Brasil.

Permitir, para fim de extração e análise de dados, o desbloqueio dos dispositivos equipados com os chipsets mais difundidos, incluindo, no mínimo: **Qualcomm, Exynos, Spreadtrum e MTK;**

Solução para extração e análise de dados a partir de serviços de computação em nuvem. Deve permitir a coleta e análise forense de dados armazenados na nuvem mediante a utilização de tokens de acesso extraídos dos aplicativos instalados nos dispositivos móveis; deve permitir a coleta e análise forense de dados armazenados na

nuvem mediante o fornecimento de credenciais de acesso (usuário e senha); deve permitir o acesso aos dados na nuvem mesmo quando exigido o duplo fator de autenticação;

Deve permitir a extração e análise de dados das principais redes sociais; extração e análise de dados dos principais aplicativos de mensageria, contemplando, no mínimo: WhatsApp, Facebook Messenger, Telegram e Signal Messenger; permitir a extração e análise dos principais serviços de armazenamentos em nuvem, contemplando, no mínimo: Dropbox, Google Backukp, Google Drive, Microsoft OneDrive, Samsung Backup e iCloud Backup.

Análise de dados de múltiplos dispositivos móveis simultaneamente, de modo a localizar vínculos entre eles. Apresentar gráficos que facilitem a identificação dos vínculos entre os usuários dos dispositivos (ligações, mensagens, localização gps, etc), considerando os aspectos temporais, de frequência, entre outros. Categorização dos dados em assuntos de relevância.

Todos os aplicativos e os acessórios da solução devem ter licença de utilização perpétua e serem atualizados durante todo período de suporte contratado; não deve haver limite de máquinas a receberem as instalações da solução; deve ser fornecido sem custo adicional todos os cabos, conectores e acessórios necessários para realizar a extração e análise de novos dispositivos suportados pela solução.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Não foram identificados outros requisitos para escolha da solução , que se trata de licenciamento de software e não de sistema/solução para tratamento de dados pessoais, afastando assim a aplicabilidade do Guia de Requisitos e Obrigações quanto a Segurança da Informação e Privacidade.

7. Estimativa da demanda - quantidade de bens e serviços

solução forense: Será adquirido apenas 1 (uma)unidade porque pretende-se contratar um único sistema que será para uso compartilhado na área requisitante.

Treinamento: Foi dimensionado uma turma de 6 alunos para comportar todos os servidores da área que precisam do treinamento.

Suporte Tecnico: Como o contrato é de 60 meses, será necessário a contratação de 5 unidades desse item (o item possui duração anual).

Serviço avançado de extração forense : Como não temos um histórico para a demanda desse serviço, estimamos de forma conservadora que será consumido uma unidade desse item por semestre, perfazendo um total de 10 unidades ao longo do contrato.

Tendo em vista necessidade de preservar o investimento realizado na solução forense , será contratado licenciamento que permite a atualização pelo período de 60 (sessenta) meses dos softwares que compõe a solução. Essa atualização é importante para manter o software compatível com os diversos dispositivos móveis que são lançados todos os anos no mercado.

8. Levantamento de soluções

Possíveis soluções:

Solução 1: Manter a infraestrutura atual ou ampliar a infraestrutura atual.

A infraestrutura de análise forense existente na DIE é precária, com apenas duas licenças do software investigativo FTK, sem direito de atualização desde 2016. A ausência de atualização inviabiliza o uso da ferramenta, pois ela se torna obsoleta, incompleta e lenta para tratar o volume e os tipos dos dados analisados nas investigações forenses.

A solução encontrada para dar continuidade aos trabalhos forenses no âmbito da DIE foi a adoção do software livre *Indexador e Pesquisador de Evidências Digitais* (IPED), desenvolvido e mantido pelo corpo funcional da Polícia Federal. A despeito de ser uma ferramenta que auxilia bastante na análise de dados convencionais (discos rígidos, caixa de e-mail, documentos etc.), é bastante limitada para trabalhos de análise de dispositivos eletrônicos portáteis. Não apresenta interfaces para a extração dos dados desses dispositivos e, também, não dispõe de ferramentas específicas para tratar os dados desses dispositivos.

Desse modo, fica explicito que a infraestrutura atual da DIE não a permite a análise forense de dispositivos eletrônicos portáteis.

Solução 2: Softwares livres (ferramentas gratuitas).

As ferramentas gratuitas, disponibilizadas por algumas empresas, como a Digital Forensics Framework (DFF), SANS Investigative Forensics Toolkit (SIFT), The Sleuth Kit, são limitadas nas extrações e análises de dados. São aplicativos isolados que não apresentam integração entre eles, não abarcando desde o desbloqueio até a análise dos dados. Cada etapa tem que ser realizada em software específico, e nem sempre tem uma boa integração com as etapas subsequentes. Carecem dos cabos, conectores e acessórios necessários para conexão com os dispositivos móveis e para a extração dos dados.

Solução 3: Aquisição de software forense.

A aquisição de software forense permitirá a extração, o processamento e a análise de dados de dispositivos eletrônicos portáteis de forma integrada. Abarcando todas etapas necessárias para uma análise forense aprofundada.

Contempla todos os cabos, conectores e plugues indispensáveis para a fase de coleta dos dados. Apresentam ferramentas para extração e tratamento de dados que estão em aplicativos específicos para dispositivos eletrônicos portáteis, e que de outro modo não são compreendidos e analisados por ferramentas forenses convencionais.

Por fim, é oportuno salientar que a aquisição de ferramenta específica atenderá à necessidade de lidar com grandes volumes e vários tipos de dados, para suprir as demandas dos trabalhos desenvolvidos atualmente pela DIE.

Levantamento de Softwares Gratuitos e Pagos disponíveis no Mercado:

8.1. Software Público (gratuito)

Não foram encontradas soluções de software no Portal de Software Público Brasileiro. O acesso ao site foi feito no dia 20/08/2021 e foi utilizada a seguinte palavra-chave no campo de busca: Forense.

https://softwarepublico.gov.br/social/search/software_infos?utf8=%E2%9C%93&utf8=%E2%9C%93&display=&filter=&software_type=public_software&query=forense&commit=Filtro

8.2. Alternativas do mercado (Pago)

Oportuno destacar que a descoberta das principais soluções disponíveis no mercado não é uma tarefa trivial. Por se tratar de ferramenta de análise forense, investigativa e voltada para os órgãos com poder de polícia, os materiais públicos disponíveis não são abundantes ou de fácil acesso.

Adiante, a empresa Gartner é referência pelos seus estudos de mercado, produzindo documentos que apontam os impactos das novas tecnologias no mundo corporativo. Relatórios como "Cool Vendors" e os gráficos do “Quadrante Mágico” são excelentes fontes de informações para descoberta das melhores empresas e dos principais produtos de tecnologia em determinado nicho de mercado.

No entanto, a busca por documentos Gartner que pudesse apontar as principais empresas e soluções no segmento de forense digital convencional ou de dispositivos móveis não se mostrou profícua. Inexistem segmentações equivalentes no Gartner, sendo a “E-Discovery” a única categoria que guarda alguma semelhança, mas não muita. Ainda assim, os documentos encontrados eram antigos e descontinuados (“deprecated”).

Nesse contexto, as soluções foram localizadas, majoritariamente, por meio de contatos realizados com os órgãos públicos federais que fazem uso desse tipo de ferramenta. Em especial o Ministério da Justiça e o Ministério Público Federal. Assim, as interlocuções realizadas serviram para elucidar quais soluções estavam em uso por esses órgãos, aquelas que obtiveram melhores resultados práticos para cada entidade governamental e os seus pontos fortes e fracos. Assim, com base nas consultas realizadas juntos a órgão de seguranças pública, ministérios públicos estaduais e federal e outras fontes, foram identificados os maiores players do mercado forense. Os quais foram elencados a seguir:

Ferramenta: Software Forensic Toolkit (FTK):

É um software desenvolvido pela AccessData, para análise forense. O seu principal foco é para análise de computadores. Assim, não apresenta interface específica para análise, extração e desbloqueio de dispositivos eletrônicos portáteis.

Atualmente a CGU detém duas licenças perpetuas de uso do FTK, sem direito de atualização. Na prática, isso representa uma grande deficiência, visto que não possibilita acesso aos novos recursos da ferramenta, deixando-a lenta, ultrapassada e obsoleta.

Ferramenta: MSAB XRY e XAMN

MSAB é uma empresa sueca relacionada com telecomunicações desde 1984. Em 2003, a empresa anunciou um software denominado XRY, destinado ao setor de forense e investigação digital de aparelhos móveis. Atualmente, conta com um portfólio amplo de softwares para desempenhar essa tarefa forense. Nesse contexto, destacam-se o XRY e o XAMN, especializados em indexação e análise, respectivamente.

O MSAB XRY e XAMN representam uma solução integrada que abarca desde os softwares, os cabos e os acessórios necessários para o desbloqueio, extração e análise de dispositivos eletrônicos portáteis. Trata-se de uma solução voltada especificamente para análise de dispositivos portáteis. As soluções trabalham de forma integrada e permitem a realização de todas as fases necessárias para a análise desses equipamentos, desde o seu desbloqueio até a análise de dados de aplicativos específicos, tais como os provenientes de redes sociais, mensageria e serviços em nuvem.

De acordo os informativos da empresa, as suas soluções utilizam um formato de arquivo proprietário (.xry), que garantem maior segurança aos dados gravados durante a extração e análise dos dados.

Ferramenta: EnCase Forensic

Tecnologia compartilhada dentro de um conjunto de produtos de investigações digitais da Guidance Software. O software vem em vários produtos projetados para uso em forense, segurança cibernética, análise de segurança e descoberta eletrônica. O EnCase é tradicionalmente usado em análise forense para recuperar evidências de discos rígidos apreendidos. É uma ferramenta muito versátil e poderosa. Contudo, não é voltada para análise de equipamentos eletrônicos portáteis, não tendo interface específica para extração, análise e desbloqueio deste tipo de equipamento. Cabe ressaltar, ainda, que é uma ferramenta com uma curva de aprendizado mais lenta, requerendo maior qualificação e treinamento por parte da equipe que a utiliza. Isso se torna especialmente importante em função da diminuta equipe de forense deste órgão de controle interno.

Ferramenta: Cellebrite UFED

Cellebrite DI é uma empresa israelense que fabrica dispositivos de extração, transferência e análise de dados para telefones celulares e dispositivos móveis. Em

2007, a Cellebrite anunciou uma linha de produtos denominada 'Universal Forensic Extraction Device' (UFED), em português 'Dispositivo Universal de Extração Forense', destinada ao setor de forense e investigação digital de aparelhos móveis.

O Cellebrite UFED é uma solução integrada que abarca desde o hardware, os softwares, os cabos e os acessórios necessários para o desbloqueio, extração e análise de dispositivos eletrônicos portáteis. Trata-se de uma solução voltada especificamente para análise de dispositivos portáteis. A sua interface integrada permite a realização de todas as fases necessárias para a análise desses equipamentos, desde o seu desbloqueio até a análise de dados específicos, tais como os provenientes de redes sociais, mensageria e serviços em nuvem.

O Cellebrite UFED destaca-se, ainda, pela ampla quantidade de equipamentos que consegue realizar análise. Abrange os principais dispositivos móveis comercializados no Brasil, incluindo o desbloqueio dos aparelhos equipados com os chipsets mais difundidos no mercado brasileiro.

Essa solução foi adquirida pelos seguintes órgãos públicos: Ministério Público do Estado do Pará, Procuradoria Geral de Justiça do Estado de Sergipe, Ministério Público do Estado do Mato Grosso do Sul, Secretaria de Estado da Segurança Pública e Defesa Social do Estado do Espírito Santo, Diretoria Técnico-Científica da Polícia Federal do Ministério da Justiça e Segurança Pública, Secretaria de Segurança Pública e Defesa Social do Governo do Estado do Ceará, Secretaria de Segurança Pública e Defesa Social do Governo do Estado do Espírito Santo, Polícia Civil do Governo do Distrito Federal e outros.

Ferramenta: Oxygen Forensic Detective

Oxygen Forensic Detective é uma plataforma de software forense integrada construída para extrair, decodificar e analisar dados de várias fontes digitais: dispositivos móveis e IoT, backups de dispositivos, UICC e cartões de mídia, drones e serviços em nuvem. O Oxygen Forensic Detective também pode encontrar e extrair uma vasta gama de artefatos, arquivos de sistema, bem como credenciais de máquinas Windows, macOS e Linux. As tecnologias implantadas no Oxygen Forensic Detective incluem, mas não estão limitadas a ignorar bloqueios de tela, localizar senhas para backups criptografados, extrair e analisar dados de aplicativos seguros e descobrir dados excluídos. Além disso, múltiplas extrações podem ser investigadas em uma única interface para obter visibilidade completa dos dados.

Ferramenta: Nuix Workstation

Nuix Workstation é uma solução para extrair inteligência de grande volume de dados estruturados, semiestruturados e não estruturados. Enquadra-se na categoria de e-Discovery – soluções que tem por objetivo permitir a descoberta de informações relevantes em grande quantidade de dados. A sua ferramenta de indexação, Nuix Engine, é famosa por ser eficiente e rápida, além de permitir a integração com várias outras ferramentas na área de forense digital – por exemplo, Relativity e Encase.

O Nuix apresenta um conjunto de funcionalidades que é muito valioso para a análise de forense digital. A capacidade de lidar com grande volume de dados, a velocidade de processamento, a categorização de uma infinidade de tipos diferentes de arquivos, o tratamento de e-mails, entre outras funcionalidades, fazem do Nuix uma ferramenta muito versátil para esse campo de atuação.

Essa solução foi adquirida pelo Conselho Administrativo de Defesa Econômica – CADE.

Contudo, é oportuno ressaltar que não é uma solução voltada para a análise de dispositivos eletrônicos portáteis. Não tem a seu dispor capacidades de desbloqueio ou extração física dos dispositivos que são de extrema relevância para esse tipo de análise forense digital. Por esse motivo, essa não é uma solução que não atende ao escopo objeto dessa contratação e por isso será desconsiderado das análises posteriores.

Avaliação das soluções identificadas frente aos requisitos

Resumo dos Requisitos		
#ID	**Nome Curto**	**Descrição**
1	Abrangência da solução	Solução forense para extração de dados e análise de equipamentos eletrônicos portáteis.
2	Extração, análise e desbloqueio	Extração, análise e desbloqueio dos principais dispositivos móveis comercializados no país, incluído os equipados com os chipsets Qualcomm, Exynos, Spreadtrum e MTK, e dos principais sistemas operacionais para smartphones.
3	Computação em nuvem (Cloud)	Solução para extração e análise de dados a partir de serviços de computação em nuvem (Cloud).
4	Análise de vínculos	Análise de múltiplos dispositivos com objetivo de identificar vínculos entre seus usuários.
5	Treinamento	Treinamento nas soluções de extração e análise de dados.
6	Atualização e garantia	Atualização e garantia das licenças pelo prazo de 60 (sessenta) meses.

7	Suporte técnico	Suporte técnico (8X5).

Requisitos de Negócio		Soluções	
#ID	Nome curto	1 - Infraestrutura atual	2 – Softwares livres
1	Abrangência da solução	Não atende	Não atende
2	Extração, análise e desbloqueio	Não atende	Não atende
3	Computação em nuvem (Cloud)	Não atende	Não atende
4	Análise de vínculos	Não atende	Não atende
5	Treinamento	Não atende	Não atende
6	Atualização e garantia	Não atende	Não atende
7	Suporte técnico	Não atende	Não atende

Requisitos de Negócio		Soluções				
#ID	Nome curto	3 – Aquisição de software forense				
		3.1 FTK	3.2 MSAB XRY	3.3 EnCase Forensic	3.4 Cellebrite UFED	3.5 Oxygen Forensic
1	Abrangência da solução	Não atende	Atende	Não atende	Atende	Atende

2	Extração, análise e desbloqueio de dispositivos móveis	Não atende	Parcialmente	Não atende	Atende	Parcialmente
3	Computação em nuvem (Cloud)	Não atende	Parcialmente	Não atende	Atende	Parcialmente
4	Análise de vínculos	Não atende	Atende	Não atende	Atende	Parcialmnete
5	Treinamento	Atende	Atende	Atende	Atende	Atende
6	Atualização e garantia	Atende	Atende	Atende	Atende	Atende
7	Suporte técnico	Atende	Atende	Atende	Atende	Atende

REQUISITOS TECNOLÓGICOS - QUADRO COMPARATIVO

Quadro comparativo entre as principais soluções de mercado para examinadores e investigadores que precisam ter acesso aos dados de dispositivos móveis e sistemas computacionais em nuvem (Cloud), para demandas em laboratório e em campo. Na tabela abaixo estão listadas apenas as soluções que atendam total ou parcialmente aos requisitos de negócio.

Funcionalidades	**UFED**	**XRY**	**Oxygen**
Funcionalidades de Desbloqueio e Extração (Física e Lógica) de Dispositivos Móveis			
Extração seletiva	**Sim**	**Sim**	**Sim**
Extração lógica de Ios	**Sim**	**Sim**	**Sim**
Extração física de Ios	**Parcial**	**NÃO**	**NÃO**
Extração lógica de Android	**Sim**	**Sim**	**Sim**
Extração através do modo EDL com descriptografia	**Sim**	**NÃO**	**NÃO**
Extração de celulares com descriptografia de chipsets MTK	**Sim**	**NÃO**	**NÃO**

Extração do tipo Smart ADB	**Sim**	**NÃO**	**NÃO**
Extração de dispositivos Samsung Qualcomm com descriptografia	**Sim**	**Parcial**	**NÃO**
Desbloqueio Android Genérico	**Sim**	**NÃO**	**NÃO**
Downgrade de APK	**Sim**	**Parcial**	**Parcial**
Extração de Huawei Kirin	**Sim**	**NÃO**	**NÃO**
Extração de LG LAF	**Sim**	**NÃO**	**Sim**
Extração Samsung ADB	**Sim**	**Sim**	**Sim**
Extração através do modo TWRP	**Sim**	**Sim**	**Sim**
Extração de celulares com chipsets CoolSand	**Sim**	**Sim**	**NÃO**
Extração de celulares com chipsets Spreadtrum	**Sim**	**Parcial**	**Sim**
Extração parcial de iPhone bloqueado via checkm8	**Sim**	**Parcial**	**Parcial**
Extração completa de iPhone desbloqueado via checkm8	**Sim**	**Parcial**	**Parcial**
Funcionalidades de Decodificação e Análise de Dispositivos Móveis			
Emulação de Android	**Sim**	**NÃO**	**NÃO**
Enriquecimento de geolocalização	**Sim**	**NÃO**	**Sim**
Recuperação de dados públicos de redes sociais	**Sim**	**NÃO**	**NÃO**
Identificação de aplicativos não suportados	**Sim**	**NÃO**	**NÃO**
Detecção de Malware	**Sim**	**NÃO**	**Sim**
Customização e execução de scripts Python	**Sim**	**Sim**	**NÃO**

Visualização de SQLite	**Sim**	**Sim**	**Sim**
Visualização de Plist	**Sim**	**Sim**	**Sim**
Visualização em formato Hexadecimal	**Sim**	**Sim**	**Sim**
Visualização em linha de tempo	**Sim**	**Sim**	**Sim**
Visualização de geolocalização em mapas	**Sim**	**Sim**	**Sim**
Suporte a conjuntos de Hash	**Sim**	**Sim**	**Sim**
Customização de relatórios	**Sim**	**Sim**	**Sim**
Filtro avançado	**Sim**	**Sim**	**Sim**
Lista de palavras-chave	**Sim**	**Sim**	**Sim**
Enriquecimento dos identificadores de BSSID de forma online ou offline para trazer endereços de redes Wireless	**Sim**	**NÃO**	**NÃO**
Tradução automática de informações de geolocalização (latitude e longitude) em endereços	**Sim**	**NÃO**	**NÃO**
Captura e gravação de telas da solução durante o processo de investigação como documentação adicional visando a complementação do relatório final	**Sim**	**NÃO**	**NÃO**
Busca por padrões de informações em bancos de dados para criação automática de parser das soluções não suportadas	**Sim**	**NÃO**	**NÃO**
Recuperação de imagens, localizações, strings e demais arquivos apagados (carving)	**Sim**	**NÃO**	**NÃO**
Descoberta de dados de forma aprimorada por meio de técnica de Heurística (AppGenie)	**Sim**	**NÃO**	**NÃO**
Tratamento de banco de dados de aplicativs não categorizados, através do banco de dados (Assistente do SQLite);	**Sim**	**NÃO**	**NÃO**

Geração de dicionário de palavras e números, para ser utilizado como referência de ataque para quebra de senha	**Sim**	**NÃO**	**NÃO**
Suporte a evidências encaminhadas através de ordem judicial por fabricantes, tais como: Apple, Instagram, Facebook, Google, Snapchat, Discord, TextNow, SkyECC	**Sim**	**NÃO**	**NÃO**
Classificação de imagem e vídeo por categorias (ex: dinheiro, placas de veículos, cartão de crédito, quartos de hotel, faturas, documentos manuscritos, documentos)	**Sim**	**NÃO**	**NÃO**
Identificação de arquivos por meio de algoritmo de HASH, incluindo suporte a banco de dados do Projeto VIC e CAID	**Sim**	**NÃO**	**NÃO**
Detecção de transações através de criptomoedas, incluindo o endereço e os dados do dispositivo	**Sim**	**NÃO**	**NÃO**
Recuperação de dados de arquivos no formato TAR sem a necessidade de descompactação	**Sim**	**NÃO**	**NÃO**
<u>Funcionalidades de Extração e Análise de Dados de Serviços Computacionais em Nuvem</u>			
Recuperação de rotas TCP/IP	**Sim**	**NÃO**	**NÃO**
Recuperação de páginas WEB	**Sim**	**NÃO**	**Sim**
Configuração de Proxy	**NÃO**	**NÃO**	**Sim**
Recuperação de dados públicos de redes sociais	**Sim**	**Sim**	**NÃO**
Localização e extração de tokens do computador (Windows e macOS)	**Sim**	**Sim**	**Sim**
Localização e extração de tokens do celular	**Sim**	**Sim**	**Sim**
Suporte fontes com duplo fator de autenticação	**Sim**	**Sim**	**Sim**
Extração não rastreável pelo usuário	**Sim**	**Sim**	**NÃO**
Captura e/ou gravação de telas	**Sim**	**NÃO**	**NÃO**

A ferramenta Cellebrite UFED, única solução técnica e funcionalmente viável que atende às necessidades da CGU, assim, não cabe apresentar análise comparativa entre as soluções. Essa ferramenta é utilizada por diversos órgãos públicos que atuam na área de investigação, demonstrando, assim, elevado nível de aceitabilidade. Por possuir elementos únicos, não identificados em outras ferramentas, a aquisição se dará por inexigibilidade de licitação, com base no art. 25, inciso I, da Lei nº 8.666/93. A solução forense UFED é desenvolvida pela empresa Cellebrite, de origem israelense. No Brasil, a Empresa TechBiz Forense Digital detém a exclusividade como representante da solução denominada UFED, fabricada pela Cellebrite.

Dentre as principais características que tornam a solução única e singular, destacam-se:

- Integração entre todas as ferramentas de extração e análise forense oferecidas pela Solução;
- Suporte às extrações de dados realizadas pelo equipamento de desbloqueio de senha;
- Suporte à integração com solução de quebra de senhas capaz de extrair dados de modelos, como: Iphones 5, 6, 6s, 7, 7s, 8, 8+ e 10 e SamSung S6, S7, S8, S9 e S10;
- Capacidade de extração de credenciais ou tokens de acesso a aplicativos na nuvem;
- Capacidade de realizar a análise de Malware;
- Capacidade de realizar extração profunda de dados, mediante solução de rooting temporário (ADB);
- Capacidade de realizar extrações de sistema de arquivos de dados de aplicativos bloqueados usando o downgrade de versões;
- Suporte ao enriquecimento de endereços BSSID e ERBS, a fim de geoposicionar os históricos de conexões do celular;
- Capacidade de realizar a extração de dados em Drones;
- Capacidade de detectar imediatamente e combinar objetos em imagens e vídeos, como armas, dinheiro, nudez, exploração infantil ou documentos;
- Capacidade de realizar foco em pessoas de interesse com reconhecimento facial automático;
- Capacidade de realizar o reconhecimento ótico de caracteres;
- Capacidade de realizar a análise ligações dentro das redes relacionadas ao caso para revelar conexões ocultas, hierarquias de grupos e padrões de comunicação;
- Capacidade de efetuar análise multicaso por pessoa, tipo de crime ou período;
- Suporte à importação de dados de Contas Reversa de operadora de Telefonia para o caso;
- Capacidade de realizar a ingestão de conteúdo de nuvem, tais como backup Icloud e Google Takeout, obtidos através de decisão judicial;
- Capacidade de realizar a ingestão de dados obtidos através de imagens de computadores no formato E01 e DD;
- Capacidade de cruzar dados de diversas fontes diferentes tais como: Celulares, ERBS, Dados de Nuvem e Computadores;

- Suporte a serviço avançado de desbloqueio ou extração de dispositivos móveis bloqueados por senha não suportados pela aplicação da solução padrão, dos fabricantes Apple e SamSung (entre outros), em laboratório próprio do fabricante, único no Brasil, com capacidade exclusiva de permitir o desbloqueio, revelação de senha, “by-pass” de senha, descriptografia, extração física e/ou file system de dispositivos celulares específicos nos sistemas operacionais iOS e Android.

9. Análise comparativa de soluções

Ferramenta: Cellebrite UFED

- Descrição da solução: Cellebrite UFED
- Fornecedores da solução: TechBiz Forense Digital é fonercedor exclusivo da solução, conforme informado na carta ABES que consta no processo.
- Quem utiliza e valor pago: Ministério Público do Estado do Pará, valor R$ 248.899,73 (Contrato nº 080/2020-MP-PA). Secretaria de Estado de Justiça e Segurança Pública do Estado do Acre, valor R$ 379.987,92 (Contrato nº 73 /2020). O valor depende do tipo de licenciamento contratado, bem como o período contratual.
- Diferentes formas de contratação:
  - Compra da licença do software.
  - Compra do direito de atualização
- Diferentes formas de pagamento:
  - Único para a compra do licencimento
- Requisitos da solução
  - Capacitação: Treinamento nas soluções de extração e análise de dados, abrangendo uma turma de até 6 alunos, com carga horária mínima de 32 horas, na modalidade presencial ou à distância – a depender das condições sanitárias do momento do treinamento. No caso de escolha da modalidade presencial, o curso deve ser realizado em Brasília/DF.
  - Legais: Não se aplica.
  - Manutenção: Suporte técnico remoto e atualização tecnológica por, no mínimo, 60 meses. incluída na contratação. O suporte técnico remoto deverá estar disponível em dias úteis, de segunda a sexta-feira, das 09h às 18h (5x8).
  - Temporais: A solução deverá ser entregue em até 15 (quinze) dias úteis.
  - Segurança: Deverá ser observada a Política de Segurança da Informação – POSIN, da CGU, instituída por meio da Portaria nº 2.042/2017, reeditada mediante a Portaria nº 587/2021.
  - Sociais, ambientais e culturais: Fornecimento de manuais em língua portuguesa.
  - Sustentabilidade: A licença de software e os manuais deverão ser entregues em formato eletrônicoa, evitando produção e transporte de mídias.
- Atendimento aos padrões e modelos do Governo Eletrônico:

	Atende	Não atende	Não se aplica
ePing			X
eMag			X
ePwg			X
ICP-Brasil			X
e-ARQ			X

- Necessidade de adequação do ambiente para implantação e operação da solução:
  - **Recursos materiais:** Não há necessidade de adequação.
  - **Recursos humanos**: Previsão de treinamento na contratação.
- Mecanismos de continuidade da solução: Renovação de licença do software, ao término do prazo da atualização (5 anos), o software precisa ser constantemente atualizado para ele acompanhar a evolução tecnológica dos dispositivos móveis existentes.

10. Registro de soluções consideradas inviáveis

As soluções 1, 2, 3.1, 3.3 mostram-se inviáveis pelo não atendimento aos requisitos de negócios 1, 2, 3 e 4.

A infraestrutura de análise forense existente na DIE, solução 1, é precária, com apenas duas licenças do software investigativo FTK, sem atualização desde 2016, ou seja, a DIE não dispõe de ferramenta forense robusta para extração, processamento e análise de equipamentos portáteis. Há limitação e demora nas coletas e análises dos dados; muitas vezes é necessário solicitar colaboração de outros órgãos públicos, fato que atrasa ainda mais o andamento e resultado dos trabalhos.

Os softwares livres, solução 2, possuem várias limitações: interface complexa, o tempo de retorno da coleta de dados é alto; a recuperação e integridade dos dados coletados em comparação à fonte dos dados são deficientes. Em especial, os softwares livres não se apresentam como uma alternativa completa, que abrange desde o desbloqueio até a análise dos dados. Não inclui os cabos, conectores, e acessórios necessários para o desbloqueio e extração dos dados dos dispositivos móveis; os vários softwares exigem treinamentos específicos; e cada etapa da investigação forense tem que ser

realizada em software específico, e nem sempre há uma boa integração com as etapas subsequentes.

Quanto a aquisição de softwares:

Ferramenta 3.1 FTK: Não atende por não ser uma solução voltada especificamente para análise forense de dispositivos eletrônicos portáteis; não dispõe de hardware, software, cabos, conectores e acessórios que permitam o desbloqueio, a extração e a análise de dados de diapositivos móveis; e não dispõe de ferramentas para extração e análise de dados de serviços em nuvem (cloud).

Ferramenta 3.2 MSAB XRY e XAMN: Após comparativo técnico na tabela acima verificou-se que esses softwares não atenderam vários itens que são essenciais para a extração e análises de dados em dispositivos móveis e serviços computacionais em nuvem.

Ferramenta 3.3 EnCase Forensic: Não atende por não ser uma solução voltada especificamente para análise forense de dispositivos eletrônicos portáteis; não dispõe de hardware, software, cabos, conectores e acessórios que permitam o desbloqueio, a extração e a análise de dados de diapositivos móveis; e não dispõe de ferramentas para extração e análise de dados de serviços em nuvem (cloud).

Ferramenta 3.4 Cellebrite UFED: atende a todos requisitos.

Ferramenta 3.5 Oxygen Forensic: Após comparativo técnico na tabela acima verificou-se que esse software não atendeu vários itens que são essenciais para a extração e análises de dados em dispositivos móveis e serviços computacionais em nuvem.

11. Análise comparativa de custos (TCO)

Análise de Custo das Soluções

Ferramenta Cellebrite UFED: R$ 726.535,22 (setecentos e vinte e seis mil, quinhentos e trinta e cinco reais e vinte e dois centavos), para o período de 60 (sessenta). A forma de pagamento será definido no termo de referência.

a) UFED 4PC (com 5 anos de atualização de software, garantia, recebimento de novos cabos e suporte)

Produto	Unidade	Qtd.	Preço Un.	Subtotal
UFED 4PC Ultimate – HW Gov	Unidade	1,00	R$ 8.343,50	R$ 8.343,50
UFED 4PC Ultimate – SW Gov	Licença de uso perpétua	1,00	R$ 83.522,45	R$ 83.522,45

UFED 4PC Ultimate – SW Renewal	Ano	4,00	R$ 43.165,98	R$ 172.663,92
Valor Total:				**R$ 264.529,87**

b) UFED Cloud Analyzer (com 5 anos de atualização de software e suporte)

Produto	Unidade	Qtd.	Preço Un.	Subtotal
UFED Cloud Analyzer Perpetual – HW Gov	Unidade	1,00	R$ 1.017,50	R$ 1.017,50
UFED Cloud Analyzer Perpetual SW Gov	Licença de uso perpétua	1,00	R$ 65.993,50	R$ 65.993,50
UFED Cloud Analyzer SW Renewal	Ano	4,00	R$ 25.351,33	R$ 101.405,32
Valor Total:				**R$ 168.416,32**

c) UFED Pathfinder Desktop – Add on Dongle (com 2* anos de atualização de software e suporte)

Produto	Unidade	Qtd.	Preço Un.	Subtotal
Pathfinder Desktop HW-Gov, Add on Dongle	Unidade	1,00	R$ 1.017,50	R$ 1.017,50
Pathfinder Desktop SW-Gov, Add on Dongle	Licença de uso perpétua	1,00	R$ 54.323,63	R$ 54.323,63
Pathfinder Desktop SW Renewal, Add on Dongle	Ano	1,00	R$ 14.057,90	R$ 14.057,90
Valor Total:				**R$ 69.399,03**

*** a forcedora indicou que esse produto será descontinuado, restando apenas mais dois anos de suporte e atualização.**

d) Treinamento para uma turma de 6 pessoas

Produto	Unidade	Qtd.	Preço Un.	Subtotal
Treinamento UFED 32h (turma de 6 alunos)	Turma	1,00	R$ 33.000,00	**R$ 33.000,00**

e) Suporte técnico remoto 8x5

Produto	Unidade	Qtd.	Preço Un.	Subtotal
Suporte Técnico remoto 8x5	Ano	5,00	R$ 7.500,00	**R$ 37.500,00**

f) Cellebrite Advanced Service - Laboratório Forense

Produto	Unidade	Qtd.	Preço Un.	Subtotal
CAS - Cellebrite Advanced Service*	Unidade	10	R$ 15.369,00	**R$ 153.690,00**

***Pagamento sob demanda.**

Os valores elencado acima foram extraídos da proposta comercial enviada pela empresa TECHBiz.

12. Descrição da solução de TIC a ser contratada

Item 1: UFED 4PC Ultimate-HW: Refere-se a porcao de hardware da solucao, incluindo ai cabos, conectores, adaptadores e demais necessarios a conexao com os dispositivos moveis e demais plataformas eletronicas portateis para, em interacao com a porcao software, proceder a extracao e analise dos dados ali constantes. Diga-se, esses elementos sao indispensaveis a operacionalizacao da solucao.

Item 2: UFED 4PC Ultimate-SW: Refere-se ao software da solucao, que permite a extracao, o processamento e a analise dos dados, com suas funcionalidades, recursos e capacidades tecnicas, especialistas em forense computacional.

item 3: UFED 4PC Ultimate-SW Renewal: Refere-se ao servico de atualizacao tecnologica fornecido pelo proprio fabricante, contratado em periodo anual, responsavel pelas correcoes, melhorias e aprimoramentos do produto, incluindo ai a

porcao hardware, com encaminhamento de novos cabos, conectores e demais, sempre que desenvolvidas novas capacidades para extracao de um novo modelo de dispositivo movel, por exemplo.

item 4: UFED Cloud Analyzer -HW: Refere-se a porcao de hardware da solucao – o dongle para acesso.

item 5: UFED Cloud Analyzer -SW: Refere-se ao software da solucao que permite a extracao, o processamento e a analise dos dados, com suas funcionalidades, recursos e capacidades tecnicas, especialistas em forense computacional.

item 6: UFED Cloud Analyzer -SW Renewal: Refere-se ao servico de atualizacao tecnologica fornecido pelo proprio fabricante, contratado em periodo anual, responsavel pelas correcoes, melhorias e aprimoramentos do produto.

Item 7: UFED Analytics Desktop (Pathfinder) -HW: Refere-se a porcao de hardware da solucao – o dongle para acesso.

Item 8: UFED Analytics Desktop (Pathfinder) -SW: Refere-se ao software da solucao, com licenciamento perpetuo, que permite o processamento e a analise dos dados, com suas funcionalidades, recursos e capacidades tecnicas, especialistas em forense computacional.

item 9: UFED Analytics Desktop (Pathfinder) -SW Renewal: Refere-se ao servico de atualizacao tecnologica fornecido pelo proprio fabricante, contratado em periodo anual, responsavel pelas correcoes, melhorias e aprimoramentos do produto.

item 10: Treinamento: Capacitação presencial para uma turma de 6 pessoas com carga horário mínima de 32h. O treinamento deverá abordar todas as funcionalidades da solução forense fornecida pela fabricante Cellebritte.

item 11: Suporte Tecnico: Fornecido por esta TechBiz Forense Digital Ltda, refere-se ao servico opcional de suporte tecnico com atendimento remoto, 8X5, de chamados relacionados a duvidas de utilizacao, erros ou falhas tecnicas na solucao, em horario comercial, cuja metrica de contratacao e anual.

item 12: CAS : Solução que será fornecida, sob demanda, o direito de uso (Voucher) do serviço avançado para desbloqueio de aparelhos dos fabricantes Apple e SamSung, entre outros, em laboratório próprio da fabricante Cellebrite, no Brasil. Esse serviço permite a CGU encaminhar ao laboratório da fabricante do software, dispositivos que a CGU não tenha conseguido extrair a analisar os dados. O laboratório da Cellebrite possui ferramentas mais especializadas que não estão sendo contratadas pela CGU. Esse serviço funciona como uma segunda estância para análise pontuais de dispositivos que a CGU não tenha conseguido analisar.

13. Estimativa de custo total da contratação

Valor (R$): 726.535,22

Conforme definido no item 11 - Análise Comparativa de Custos (TCO)

14. Justificativa técnica da escolha da solução

De acordo com os itens 8 e 9 a única solução tecnicamente viável é o UFFED Cellebrite.

15. Justificativa econômica da escolha da solução

Das soluções forenses apresentadas, houve apenas uma viável, pois atendeu aos requisitos técnicos e de negócios. Logo, não houve um critério econômico na escolha da solução, mas apenas critérios técnicos e de negócios. Ressalta-se que há orçamento suficiente para a contratação.

16. Benefícios a serem alcançados com a contratação

Com a aquisição do solução de análise forense que se pretende contratar, a CGU irá atingir os seguintes objetivos: construir um ambiente computacional adequado, garantindo eficiência nas investigações; Aprofundamento nas investigações, por meio da análise dos dados obtidos de aparelhos celulares; além de, aumentar a capacidade operativa do Órgão.

Cabe à Coordenação-Geral de Inteligência de Dados – CGDATA as atividades de análise forense computacional em material eletrônico, com vistas a subsidiar investigações, executadas pela própria CGU, e operações especiais, realizadas em conjunto com a Polícia Federal (PF); Ministérios Públicos Federal e Estaduais; Receita Federal do Brasil (RFB); Polícia Rodoviária Federal (PRF); Grupos de Atuação Especial de Combate ao Crime Organizado nos Estados; e Polícias Civis nos Estados. A estrutura forense atual é bastante limitada, e não possui ferramentas para extração e análise de dados a partir de dispositivos eletrônicos portáteis e em nuvem. Daí a necessidade da aquisição de uma solução forense, com tais especificidades, para suprir essa lacuna. Atualmente, a demanda no que se refere a análise em equipamentos eletrônicos, como, computadores, notebooks, smartphones, drivers externos, tem aumentado. As soluções pesquisadas no mercado não possuem, em sua maioria, funcionalidades que auxiliem nas atividades específicas de serviço de inteligência da CGU. Assim, a aquisição de ferramenta robusta e eficiente para examinar dispositivos móveis e dados em nuvem é essencial.

17. Providências a serem Adotadas

Não há nenhuma providencia ou necessidade de adequação da infraestrutura do Órgão para viabilizar a execução contratual.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Consoante o inciso V do art. 11 da Instrução Normativa n° 1 de 4 de abril de 2019, da SGD/ME, esta equipe de planejamento, instituída pelo Ato de Designação DGI 2032943, de 20/07/2021, declara viável esta contratação com base neste Estudo Técnico Preliminar.

19. Responsáveis

DEMÉTRIUS BATISTA BORGES

Integrante Técnico

GUTEMBERG ASSUNÇÃO VIEIRA

Intergrante Requisitante

Declaro que o conteúdo do presente documento está adequado às disposições da Instrução Normativa nº 01/2019 – SGD/ME.

HENRIQUE APARECIDO ROCHA

Autoridade Máxima de TIC