

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**„ Zakup aktualizacji licencji oprogramowania dla potrzeb jednostek Policji garnizonu mazowieckiego”****ZADANIE NR 1**

1. Aktualizacja licencji na oprogramowanie Magnet AXIOM (1 - licencja) Nr klucza licencji: B20241108000971 wraz ze świadczeniem 12 miesięcznego wsparcia technicznego.

1.	Zaawansowane narzędzie do analizy z zakresu informatyki śledczej	<ul style="list-style-type: none"> Obsługa systemów operacyjnych: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OSX, iOS, Android, Kindle Fire; Obsługa systemów plików: NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT; Natywne wsparcie dla formatów obrazów E01, Ex01, L01, Lx01, AD1, dd, raw, bin, img, ima, dmg, flp, vfd, bif, vmdk, vhd, vdi, xva, zip, tar; Dwie osobne aplikacje, Examine do przeprowadzania badań, Process do przetwarzania dowodów; Dodatkowe moduły umożliwiające wyszukiwanie dokumentów aplikacji biznesowych oraz artefaktów systemów operacyjnych jak również artefaktów z urządzeń mobilnych; Wyszukiwanie istniejących i usuniętych artefaktów na dysku twardym oraz w zrzutach pamięci RAM, kopiach volume shadow, fizycznych i logicznych obrazach urządzeń mobilnych, pojedynczych plikach i folderach; Wyodrębnianie historii komunikacji w portalach społecznościowych, czatach IM (Instant Messaging), artefaktów znajdujących się w chmurze, danych aplikacji służących udostępnianiu plików P2P, danych kopii zapasowych urządzeń mobilnych, skrzynek pocztowych, historii przeglądarek internetowych, plików graficznych oraz wideo; Wykrywanie szyfrowanych nośników za pomocą Truecrypt, Bitlocker, PGP oraz Safeboot; Techniki wyodrębniania danych pozwalające na lepsze odzyskiwanie danych z przestrzeni niezalokowanej i pamięci RAM.
2.	Wsparcie techniczne Oferenta	<ul style="list-style-type: none"> Dostęp do aktualizacji oprogramowania przez okres wsparcia; Telefoniczną oraz mailową pomoc techniczną w diagnozowaniu i usuwaniu usterek oraz nieprawidłowości w działaniu programu oraz wskazywanie rozwiązań zastępczych; Konsultacje merytoryczne w języku polskim; Możliwość zgłaszania awarii oprogramowania w języku polskim.

2. Aktualizacja licencji na oprogramowanie UFED 4 PC (1 - licencja) Nr klucza licencji: 5885 430792732 z UPGARDE do Inseyets Online Pro (UFED 4PC Ultimate + ekstrakcje FFS, CLAS, Device Triage, Cloud Extraction, Comander Upgraded Inseyets KIT) wraz ze świadczeniem 12 miesięcznego wsparcia technicznego.

1.	Zaawansowane narzędzie do ekstrakcji danych z urządzeń mobilnych	<ul style="list-style-type: none"> Oprogramowanie umożliwiające usuwanie zabezpieczeń (pattern lock, hasło, PIN) z popularnych urządzeń mobilnych, a następnie wykonywanie ekstrakcji danych tj. logiczna, systemu plików, pełny system plików, fizyczna, jak również wykonywanie zrzutów ekranu
----	--	---

		<p>prosto z włączonego urządzenia mobilnego. Dodatkowo umożliwi ekstrakcji danych z kart SIM, kart pamięci, dronów, nawigacji GPS oraz danych z chmury.</p> <ul style="list-style-type: none"> • Oprogramowanie umożliwi dodatkowo odzyskiwanie usuniętych danych. W przypadku braku profilu danego urządzenia mobilnego, oprogramowanie powinno posiadać ogólne profile dla procesorów lub systemów operacyjnych, za pomocą których umożliwia ekstrakcję danych lub obejście blokady użytkownika. • Oprogramowanie umożliwi uzyskanie wszystkich typów informacji, takich jak: <ul style="list-style-type: none"> a) wykonywanie ekstrakcji (Full File System – pełnego systemu plików) w przypadku urządzeń opartych o procesor Kirin, MTK, Qualcomm, Exynos, b) w przypadku najnowszych zabezpieczonych kodem użytkownika telefonów, oprogramowanie powinno umożliwiać obsługę tych urządzeń znajdujących się zarówno na standardowej liście wspieranych modeli, jak również – w przypadku urządzeń spoza tej listy lub urządzeń zabezpieczonych w sposób określany przez producenta jako „premium” – umożliwiać wykupienie odpowiednich kredytów, które pozwolą na realizację procesu pozyskiwania danych, obejmującego m.in. obejście zabezpieczeń systemowych, ekstrakcję fizyczną, logiczną lub plikową, oraz deszyfrowanie zawartości urządzenia, c) szybkie pozyskanie i zabezpieczenie danych w trybie wstępnej analizy (triage), bez konieczności pełnej ekstrakcji zawartości urządzenia. Dane pozyskane w tym trybie powinny być automatycznie archiwizowane w sposób nienaruszający ich integralności oraz umożliwiać ich dalszą analizę w środowisku laboratoryjnym. Wskazane jest, aby dane te były zapisywane w formacie umożliwiającym walidację integralności (np. poprzez sumy kontrolne MD5, SHA lub inne mechanizmy kryptograficzne), d) pozyskiwanie danych z usług przechowywania w chmurze (np. iCloud, Google, Microsoft, WhatsApp Cloud, Facebook Cloud) na podstawie legalnie uzyskanych danych uwierzytelniających (loginy, hasła, tokeny, pliki autoryzacyjne). Pozyskane dane powinny być zabezpieczone w sposób zapewniający integralność i autentyczność, z możliwością wygenerowania raportu z czynności pobrania, zawierającego m.in. datę, zakres i źródło danych, e) rejestry połączeń głosowych i transmisji danych, obejmujące połączenia wychodzące, przychodzące i nieodebrane, zarówno realizowane przez tradycyjną sieć operatora (CS/PS), jak i za pośrednictwem sieci internetowej (VoIP, połączenia w komunikatorach internetowych), f) listy zadań i przypomnień zarejestrowanych lokalnie na urządzeniu lub w powiązanych aplikacjach, g) kalendarze i terminarze spotkań, h) wiadomości tekstowe i multimedialne, w tym: wiadomości SMS, EMS, MMS, wiadomości e-mail (wraz z załącznikami), wiadomości pochodzące z aplikacji komunikatorów internetowych (np. WhatsApp, Signal, Telegram, Messenger, Viber, Skype, TikTok, Instagram, z zachowaniem informacji towarzyszących, takich jak metadane, załączniki, status doręczenia, czas wysłania i odbioru, i) pliki multimedialne z pamięci urządzenia (w tym z folderów aplikacji), obejmujące pliki graficzne (JPG, PNG, HEIC itd.), audio (MP3, AAC, WAV itd.) oraz wideo (MP4, AVI, MOV itd.), z
--	--	---

		<p>możliwością przeglądu miniatur, metadanych EXIF oraz analizy powiązań aplikacyjnych,</p> <p>j) automatyczną kategoryzację plików multimedialnych pozyskanych z urządzenia (w tym plików graficznych oraz plików z zapisem wideo) z wykorzystaniem algorytmów rozpoznawania treści. Klasyfikacja powinna obejmować m.in. wykrywanie twarzy, dokumentów, pisma odręcznego, broni, narkotyków, papierosy, tatuaże, treści o charakterze seksualnym (w tym CSAM – Child Sexual Abuse Material), nagich ciał, pojazdów, oraz innych istotnych kategorii wspierających wstępną ocenę dowodów. Powinien być dostępny mechanizm filtrowania, grupowania oraz wizualizacji danych w oparciu o przypisane kategorie oraz metadane plików,</p> <p>k) pliki baz danych wykorzystywanych przez system operacyjny oraz aplikacje użytkownika (np. SQLite, Realm), z możliwością ich podglądu, dekodowania oraz eksportu do dalszej analizy,</p> <p>l) historię aktywności internetowej, obejmującą przeglądane adresy URL, historię wyszukiwania, zakładki oraz pobrane pliki – zarówno z poziomu systemowej przeglądarki, jak i przeglądarek aplikacji zewnętrznych,</p> <p>m) dane geolokalizacyjne, w tym lokalizacje pochodzące z danych systemowych, historii Google/Apple, tagów EXIF, usług mapowych oraz aplikacji trzecich – prezentowane na mapie i w formie tabelarycznej,</p> <p>n) listę zainstalowanych aplikacji, w tym identyfikacja aplikacji potencjalnie złośliwych (malware, spyware, stalkerware), z możliwością analizy śladów ich działania oraz chronologii instalacji i uruchomień,</p> <p>o) identyfikację obecności złośliwego oprogramowania (malware). Powinno być dostępne automatyczne skanowanie systemu plików oraz folderów aplikacji pod kątem znanych sygnatur, heurystyk charakterystycznych dla oprogramowania szkodliwego. Wskazane jest, aby narzędzie uwzględniało aktualną bazę zagrożeń oraz pozwalało na generowanie raportów dotyczących wykrytych nieprawidłowości,</p> <p>p) identyfikację aplikacji i danych związanych z przechowywaniem i zarządzaniem aktywami kryptowalutowymi, w tym portfeli mobilnych (np. Trust Wallet, MetaMask, Exodus, Binance, Coinomi, Ledger Live Mobile), danych kluczy prywatnych, adresów publicznych, seedów oraz transakcji,</p> <p>q) eksport danych oraz generowanie raportów, w tym możliwość tworzenia raportów śledczych w formatach: XLSX, PDF, HTML oraz innych powszechnie wykorzystywanych, z możliwością selekcji danych do eksportu i dołączania podpisów cyfrowych,</p> <p>r) generowanie plików wynikowych w sposób potwierdzający integralność danych i zgodność z procedurami zabezpieczenia materiału dowodowego,</p> <p>s) obsługę projektów w formacie „.ufdx”, umożliwiającą otwieranie i analizę projektów pochodzących z innych urządzeń analizujących, zgodnych z formatem plików wykorzystywanym w systemach obecnie stosowanych w jednostkach Policji (np. UFED/Physical Analyzer).</p> <p>Wsparcie dla urządzeń min.: Android, iOS, Windows Phone. Do oprogramowania dodane będą wszystkie niezbędne akcesoria, kable, przejściówki dołączane przez producenta oprogramowania,</p>
--	--	---

		<p>wspierające proces zabezpieczania oraz pozyskiwania danych z urządzeń mobilnych, kompatybilny z oferowanym oprogramowaniem. Zestaw powinien być fabrycznie nowy, w walizce transportowej zgodny z wymaganiami producenta oprogramowania oraz zapewniać obsługę urządzeń zgodnie z aktualną listą kompatybilności. Dodatkowo powinien być wyposażony w:</p> <p>1) moduły zabezpieczające transmisję danych sieciowych (np. data blockers, osłony transmisji radiowej typu Faraday),</p> <p>2) zestaw narzędzi technicznych do bezpiecznego demontażu kart SIM, kart pamięci oraz obsługi urządzeń z uszkodzonymi portami,</p>
2.	Wsparcie techniczne Oferenta	<ul style="list-style-type: none"> • Dostęp do aktualizacji oprogramowania przez okres wsparcia; • Telefoniczną oraz mailową pomoc techniczną w diagnozowaniu i usuwaniu usterek oraz nieprawidłowości w działaniu programu oraz wskazywanie rozwiązań zastępczych; • Konsultacje merytoryczne w języku polskim; • Możliwość zgłaszania awarii oprogramowania w języku polskim.

Termin realizacji:

Dostarczenie przedmiotu zamówienia należy przeprowadzić w maksymalnym terminie do 28.05.2026 r.