**Załącznik nr 2.9 do PPU - Opis przedmiotu zamówienia dla części 9 postepowania**

**ZAKUP OPROGRAMOWANIA DO POZYSKIWANIA DANYCH Z URZĄDZEŃ MOBILNYCH i PC ORAZ ANALIZY DANYCH – 1 szt.**

|  |  |
| --- | --- |
| **Właściwości** | * Wspierane systemy operacyjne: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OSX, iOS, Android, Kindle Fire. * Wspierane systemy plików: NTFS, APFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2. * 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 oddzielne aplikacje, jedna do przeprowadzenia badań i druga do analizy. * Dodatkowe moduły umożliwiające wyszukanie dokumentów aplikacji biznesowych oraz artefaktów systemu operacyjnego 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 telefonów komórkowych, pojedynczych plikach i folderach. * Wyodrębnianie historii komunikacji w portalach społecznościowych, czatach IM (Instant Messaging), artefaktów znajdujących się w chmurze (na podstawie danych badanego urządzenia: keychain, keystore, userpermition), danych aplikacji służących udostępnianiu plików P2P, danych z kopii zapasowych telefonów komórkowych, skrzynek pocztowych, historii przeglądarek internetowych, plików graficznych oraz wideo. * Wykrywa szyfrowane nośniki za pomocą Truecrypt, VeraCrypt, Bitlocker, PGP oraz Safeboot. * Firmowe techniki wyodrębniana danych pozwalające na lepsze odzyskiwanie danych z przestrzeni niezalakowanej i pamięci RAM. * Odzyskiwanie danych z urządzeń z systemem iOS i Android poprzez artefaktowe pierwsze podejście dla najpopularniejszych aplikacji. * Wykonywanie obrazów z urządzeń mobilnych z systemem iOS i Android. * Deszyfrowanie aplikacji przy wykorzystaniu danych z keychain i keystore. * Obsługi ekstrakcji oparta na kategoriach. * Pobieranie i analizowanie danych z urządzeń z systemem Windows, Mac, Chromebook i Linux z podejściem opartym na artefaktach. * Wsparcie/obsługa niezaszyfrowanych obrazów wykonanych w innych programach/narzędziach do informatyki śledczej. * Możliwość importowania danych z różnych narzędzi (Ufed, XRY, GrayKey) oraz metod pozyskiwania danych (JTAG, ISP, ekstrakcja chipów). * Możliwość importowania danych z wielu źródeł takich jak PC, chmura, IoT czy pojazdy do jednego pliku sprawy. * Pozyskiwanie i analiza danych z platform mediów społecznościowych i usług w chmurze, a także pobieranie uprawnień i archiwów generowanych przez użytkownika, z takich źródeł jak Google, Apple, Microsoft, Facebook i innych na podstawie keychain i keystore wyodrębnionych z badanego urządzenia. * Pobieranie i analiza danych o pojazdach, m. in. z ekstrakcji Berla iVe, oraz nanoszenie danych geolokalizacyjnych i innych zdarzeń na mapę świata. * Korelacja danych pomiędzy pojazdami i innymi źródłami, które gromadzą dane geolokalizacyjne, jak np. urządzenia mobilne. |
| **Analiza** | * Automatyczna wizualizacja relacji pomiędzy artefaktami, plikami i urządzeniami przedstawiona na osi czasu. * Analiza tekstu pod kątem wyszukiwania treści o zabarwieniu erotycznym. * Szybka identyfikacja zdefiniowanych słów kluczowych dotyczących obszarów zainteresowania dla danej sprawy. * Szczegółowe podsumowanie analizy i raportowanie błędów. * Możliwość tworzenia szablonów raportów. * Możliwość swobodnego tworzenia i dopasowywania raportów. * Wbudowane narzędzia/moduły analityczne. * Optyczne rozpoznawanie znaków (OCR) zoptymalizowane do wyodrębniania tekstu z plików PDF, zeskanowanych dokumentów, obrazów dokumentów i innych obrazów, które mogą być zawarte w wiadomościach e-mail. * Natywne wsparcie analizy dowodów ze wskazanych źródeł w jednym pliku sprawy. * Sprawdzanie danych w poszukiwaniu nieznanych/potencjalnych baz danych i tworzenie z tych danych artefaktów. * Zastosowanie technologii uczenia maszynowego w celu wykrywania dowodów. * Automatyczne odszyfrowywanie poprzez wykorzystanie i pobieranie tokenów i łańcuchów kluczy z urządzeń mobilnych. * Wyszukiwanie obrazów na podstawie treści (CBIR) oraz uczenie maszynowe do przeszukiwania obrazów i tekstu. * Analiza archiwów takich jak np. Google Takeout, Facebook Download Your Information oraz inne. |
|  |  |

**DODATKOWO DLA PRZEDMIOTOWEGO OPROGRAMOWANIA :**

Roczny dostęp online do pakietu autorskich szkoleń producenta oprogramowania w zakresie minimalnym zgodnie z listą tematyczną szkoleń

* Podstawy informatyki śledczej komputerów
* Zaawansowana informatyka śledcza komputerów
* Zaawansowana informatyka śledcza urządzeń mobilnych
* Badanie incydentów komputerowych
* Badanie komputerów z system macOS
* Zbieranie i badanie danych z Internetu i tzw. chmury
* Analiza systemu plików iOS

Szkolenia powinny być realizowane online z instruktorem lub do online do samodzielnego szkolenia, w terminie wybranym przez Zamawiającego z listy dostępnych terminów wskazaną przez producenta oprogramowania w ciągu roku od dnia zakupu.

1. Wymagania w zakresie licencji.

Zamawiający wymaga, aby oferowany przedmiot zamówienia objęty był:

* + licencja musi być nowa, nie może być używana albo odnawiana,   
    i nieaktywowana nigdy wcześniej na inny urządzeniu,
  + musi istnieć możliwość przenoszenia licencji między stanowiskami,
  + nie dopuszcza się oprogramowania do zastosowań domowych,
  + **licencja musi być czasowa** **(subskrypcja) na okres 36 miesięcy począwszy od dnia dostawy (podpisania przez Zamawiającego protokołu odbioru stanowiącego załącznik nr 3 do umowy),**
  + licencja musi zostać zarejestrowana na dane Centralnego Biura Zwalczania Cyberprzestępczości – Zarząd we Wrocławiu
  + wersja instalacyjna oprogramowania musi być udostępniona na autoryzowanej stronie producenta oprogramowania,
  + w przypadku licencji elektronicznej, licencja musi zostać wysłana na adres [licencje@cbzc.policja.gov.pl](mailto:licencje@cbzc.policja.gov.pl),
  + aktywacja oprogramowania powinna umożliwiać aktywację na komputerach niepodłączonych do Internetu,
  1. Dostarczone urządzenia powinny być nowe, wolne od wad i zgodne z poziomem technologii istniejącym w momencie podpisania umowy.

………………………………………….

(podpis)