1. Oprogramowanie do wyodrębniania i analizy artefaktów internetowych, dokumentów aplikacji biznesowych, danych systemowych

|  |  |
| --- | --- |
| Funkcje użytkowe | Analiza zawartości internetowej, telefonów komórkowych, danych aplikacji, danych systemów operacyjnych, danych Internet of Things, danych znajdujących się w chmurze |
| Wsparcie dla systemów operacyjnych | Windows (wszystkie wersje), macOS, LINUX (wszystkie dystrybucje), IOS, Android, Windows Phone, Blackberry, Kindle Fire, wsparcie dla systemów Internet of Things |
| Wsparcie dla systemów plików | DOS/ Windows, UNIX/Linux, APFS oraz HFS+ |
| Wsparcie dla formatów plików | E01, L01, DD, TAR, RAW, BIN, IMG, pliki systemów wirtualnych, |
| Analiza danych | * wyszukiwanie istniejących i usuniętych artefaktów na nośnikach, obrazach i kopiach binarnych nośników, w zrzutach pamięci RAM, kopiach volume shadow, kopiach logicznych i fizycznych telefonów komórkowych, pojedynczych plikach i folderach mające na celu wyodrębnienie oraz wykonanie: * historii przeglądarek internetowych w postaci danych odwiedzanych stron, cookies, formularzy internetowych, haseł, dla przeglądarek Chrome, Firefox, Opera, Edge, Internet Explorer i innych * danych z historii portali społecznościowych Facebook, Instagram, Snapchat, Twitter i kategoryzowanie ich na poszczególne portale, * analizy zawartości czatów i komunikatorów internetowych oraz możliwość przedstawienia ich w postaci tzw. „dymków” * akwizycji danych znajdujących się w chmurach danych za pośrednictwem haseł oraz znajdowanie poświadczeń logowania do chmury na badanych nośnikach i logowanie za pośrednictwem tych poświadczeń * danych aplikacji służących do wymiany plików tzw. P2P następujących typów: Ares; Bitcoin; Cryptocurrency; eMule; Frostwire; Gigatribe; Limerunner; Limewire; Luckywire; Shareaza; Torrent; Usenet * analizy artefaktów pochodzących z systemów Windows, Linux oraz macOS wraz z elementami odzyskanymi * danych z telefonów komórkowych w postaci kontaktów, rejestru połączeń, wiadomości SMS i z komunikatorów, plików graficznych, video i audio, plików systemowych, historii internetowej przeglądarek w wersji mobilnej * danych z poczty elektronicznej przechowywanych w czytnikach poczty oraz stronach www, * wyodrębnianie dokumentów biurowych i finansowych w formatach MS Office OpenOffice i innych * wyodrębnianie danych i logów systemów operacyjnych * wyodrębnianie plików graficznych i wideo wraz z metadanymi |
| Właściwości | * pełna akwizycja danych nośników fizycznych i pamięci RAM, * Odczyt oraz analiza obrazów/zrzutów urządzeń mobilnych (iOS, Windows Mobile, Android) * odszyfrowanie systemu plików FileVault2 oraz odzysk artefaktów systemów macOS * akwizycja danych z chmur Google, WhatsApp, iCloud, Google, Facebook, Twitter, Instagram, Microsoft Office 365, Dropbox, IBM Cloud Storage, MEGA i innych * kategoryzowanie wyodrębnionych danych w postaci poszczególnych artefaktów, * wyszukiwanie słów kluczowych metodą słownikową i wyrażeń regularnych, * filtrowanie wyodrębnionych danych za pomocą różnych kryteriów, w tym za pośrednictwem wyrażeń regularnych * tworzenie graficznej wizualizacji systemu połączeń dla wyodrębnionych artefaktów * możliwość odbudowy stron www * możliwość prezentacji podsumowania analizy minimum w formacie PDF, HTML i XLS, * możliwość wyeksportowania wyodrębnionych danych do dalszej analizy w postaci sprawy typu „portable” |
| Dodatkowe wsparcie | Minimum 4 lata, liczone od dnia następnego po zakończeniu podstawowego wsparcia. |
| Uwagi | Oprogramowanie powinno być dostarczone w najnowszej wersji dostępnej w dniu dostarczenia. Zamawiający przyjmuje, że wykonawca zapewnia wraz z oprogramowaniem roczne wsparcie. Oprogramowanie powinno być dostarczone w wersji językowej obowiązującej w kraju zamawiającego lub z możliwością wyboru takiej opcji językowej zawartej we właściwościach programu o ile taka wersja występuje na rynku. W przypadku braku takiej wersji oprogramowania program powinien być w wersji angielskiej. |