AXIOM to narzędzie używane przez firmy, jednostki dochodzeniowe, wojsko i wywiad. Program

zaprojektowany jest tak by wyodrębniać i odzyskiwać artefakty internetowe, artefakty urządzeń mobilnych, dokumenty aplikacji biznesowych oraz artefakty systemowe.

Axiom zbudowany jest z dwóch aplikacji: AXIOM Process oraz AXIOM Examine.

Axiom Examine to aplikacja za pomocą, której specjalista wykona natychmiastowe kroki celem zbadania wykonanych odczytów. Narzędzie radzi sobie z wszystkimi rodzajami plików, odzyskuje i składa informacje z artefaktów, systemu plików czy rejestru.

Na uwagę w aplikacji Axiom Examine zasługuje funkcjonalność obróbki plików RAW, w tym możliwość eksplorowania systemu plików, rejestru, sprawdzania lokalizacji danych źródłowych i artefaktów w kilka sekund oraz ,,source linking", który w szybki sposób umożliwia łączenie wybranych informacji z dostępem w systemie plików lub rejestrze oszczędzając przy tym cenny czas. Aplikacja zyskała również ulepszone wyszukiwanie, sortowanie i filtrowanie danych, w tym słowa kluczowe wraz z ich podświetlaniem w wynikach, datownik, tagi, komentarze. lnterfejs programu w łatwy sposób umożliwia wyświetlanie danych w różnych widokach w tym m.in.: wyświetlanie konwersacji chat, mapa świata oraz oś czasu.

Axiom Process to aplikacja do wykonania analizy dowodów. Aplikacja umożliwia stworzenie pojedynczego pliku sprawy dla wielu dowodów, teraz biegły nie musi tworzyć dla każdego dowodu osobnej sprawy celem jego przetworzenia, gdyż możliwe to jest dla wielu dostarczonych danych w jednym czasie. Narzędzie efektywniej wykorzystuje zaimplementowane funkcjonalności celem pozyskiwania i przetwarzania obrazów ze smartfonów, dysków twardych czy innych nośników.

Axiom Process został wyposażony w innowacyjny system przetwarzania, który umożliwia szybkie wyszukiwanie oraz posiada zintegrowane widoki i filtry w tym możliwości hasowania plików celem ich przeliczania dla uproszczonej weryfikacji. Odzyskane artefakty są indeksowane przez co Axiom Examine szybciej dostarcza filtrowane lub wyszukiwane informacje. Aplikacja umożliwia również tworzenie własnych definicji dla pozyskiwania większej ilości artefaktów bez szczególnej wiedzy programistycznej.

Funkcjonalności:

- 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, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2

- Natywne wsparcie dla formatów obrazów E01, ExO1, L01, Lx01, AD1, dd, raw, bin, img, ima, dmg, flp, vfd, bif, vmdk, vhd, vdi, xva, zip, tar

- Dwie osobne aplikacje, Examine do przeprowadzenia badań oraz Process do przetwarzania dowodów

- Dodatkowe moduły umożliwiające wyszukanie dokumentów aplikacji biznesowych oraz artefaktów system operacyjnego jak również artefaktów z urządzeń mobilnych

- Wyszukuje istniejące i usunięte artefakty na dysku twardym oraz w zrzutach pamięci RAM, kopiach volume shadow, fizycznych i logicznych obrazach telefonów komórkowych, pojedynczych plikach i folderach

- funkcjonalność obróbki plików RAW, w tym możliwość eksplorowania systemu plików, rejestru, sprawdzania lokalizacji danych źródłowych i artefaktów w kilka sekund oraz ,,source linking", który w szybki sposób umożliwia łączenie wybranych informacjiz dostępem w systemie plików lub rejestrze

- ulepszone wyszukiwanie, sortowanie i filtrowanie danych, w tym słowa kluczowe wraz z ich

 podświetlaniem w wynikach, datownik, tagi, komentarze

- lnterfejs programu w łatwy sposób umożliwia wyświetlanie danych w różnych widokach w tym m.in.: wyświetlanie konwersacji chat, mapa świata oraz oś czasu

- umożliwia stworzenie pojedynczego pliku sprawy dla wielu dowodów

- Wyodrębnia historię komunikacji w portalach społecznościowych, czatach lM (lnstant Messaging), artefakty znajdujących się w chmurze, dane aplikacji służących udostępnianiu plików P2P, dane z kopii zapasowych telefonów komórkowych, skrzynek pocztowych, historii przeglądarek internetowych, plików graficznych oraz wideo,

- Możliwość wyszukiwania danych: ponad 265 artefaktów,

- Wykrywa szyfrowane nośniki za pomocą Truecrypt, Bitlocker, PGP oraz Safeboot

- Firmowe techniki wyodrębniana danych pozwalające na lepsze odzyskiwanie danych z przestrzeni niezalakowanej i pamięci RAM

- przeszukuje dyski logiczne i fizyczne,

- Możliwość przeszukiwania wieIu folderów, dysków bądź plików obrazów równocześnie

- Możliwość odbudowania stron internetowych

- szczegółowe kategoryzowanie wyodrębnionych danych,

- Możliwość wyszukiwania słów kluczowych w wynikach wyszukiwania.

- Możliwość prezentacji podsumowania analizy w formacie HTML, PDF, Excel, CSV, XML

- Możliwość wyodrębnienia sprawy do przeglądu dla osób nieposiadających licencji programu (portable Case)