Rola informatyki śledczej w rozwiązywaniu zagadek kryminalistycznych

Autor:

Bernadetta Stachura-Terlecka

BERNADETTA
STACHURA – TERLECKA

Definicja

Informatyka Śledcza to jedna z dziedzin nauk sądowych mająca na celu dostarczyć dowodów cyfrowych na popełnione przestępstwa lub nadużycia nie tylko komputerowe.

BERNADETTA
STACHURA – TERLECKA

Definicja dowodu elektronicznego

„Dowód elektroniczny to informacje zapisane na nośnikach posiadające cechy charakterystyczne i przez to wymagające specjalnego podejścia.”

Cechami charakterystycznymi dowodu, a zarazem jego wadami i zaletami są:

- Możliwość klonowania nośników,
- Ostatnią cechą dowodu elektronicznego jest rozproszenie.
- Duża łatwość modyfikacji informacji elektronicznej,

BERNADETTA
STACHURA – TERLECKA

Zastosowanie informatyki śledczej.

Informatyka śledcza ma swoje zastosowanie nie tylko w przypadku przestępstw komputerowych ale również w tradycyjnych przestępstwach. W przypadku tradycyjnych przestępstw możemy wyróżnić trzy typy spraw:

- Sprawy z powództwa cywilnego,
- Sprawy kryminalne,
- Sprawy o przestępstwa skarbowe.

BERNADETTA STACHURA – TERLECKA

Problemy spotykane podczas analizy urządzeń

- Lokalizacja telefonu komórkowego na podstawie jego użytkowania,
- nowe struktury i systemy plików, usługi przechowywania danych, urządzenia peryferyjne, złącza czy kable,
- Pojemność urządzeń rośnie, dzięki zapotrzebowaniu na coraz mocniejsze urządzenia typu „mini komputer”,
- Nie tylko typy danych ewoluują, ale także sposób, w jaki urządzenia mobilne są wykorzystywane,
- Czas potrzebny na analizę dysków twardych komputera,
- Szyfrowane systemy plików,
- Systemy synchronizowane (chmury np. apple).

Typu przejęcia danych informatyce śledczej

- Pozyskanie ręczne,
- Pozyskanie logiczne,
- Przejęcie systemu plików,
- Fizyczne przejęcie,

BERNADETTA STACHURA – TERLECKA

Przykłady oprogramowania wykorzystywanego w informatyce śledczej.

Oprogramowanie służące do robienia zrzutów pamięci ulotnej:

- LiME,
- /dev/Cash,
- Mac Memory Reader,
- ForensicToolkit (FTK),
- Win32dd ,
- Windows Memory Reader,
- En-case,
- Helix,
- X-Ways,

Oprogramowanie służące do analizy dysków to między innymi:

- Internet Examiner 3.8.18 (niestety wersja demo nie radzi sobie z wyszukiwaniem danych na dyskach powyżej 80GB i po kilku godzinach działania zawiesza się),
- Internet Evidence Finder v6.0 (sposób działania pokazany jest w części praktycznej dotyczącej analizy Social Forensic).

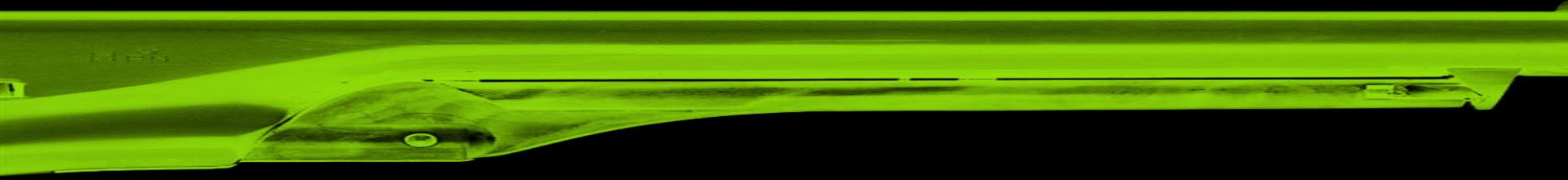
Oprogramowanie służące do analizy urządzeń mobilnych:

- Micro Systemation XRY,
- MOBILedit! Forensic,

BERNADETTA
STACHURA – TERLECKA

DOBRE PRAKTYKI

BERNADETTA
STACHURA - TERLECKA



Informatyka śledcza jak i inne gałęzie nauk sądowych jest dziedziną mającą na celu dostarczenie dowodów przy czym dowody te mają czysto charakter danych elektronicznych. Aby jednak móc mówić o dobrych praktykach w rozumieniu zbierania, analizowania, przechowywania i niszczenia dowodów elektronicznych należy zdefiniować czym taki dowód jest.

BERNADETTA
STACHURA – TERLECKA

Dobre praktyki

Wszystkie zasady zawarte w dobrych praktykach pokazują w jaki sposób zadbać o dwie najważniejsze cechy dowodu elektronicznego czyli o wierność i autentyczność. Wierność dowodu elektronicznego to możliwość sprawdzenia czy materiał w czasie analiz i zabezpieczania nie został zmieniony. Autentycznością zaś nazywamy bezsporność co do źródła pochodzenia dowodu elektronicznego.

- Każdy zabezpieczony sprzęt (w tym nośnik danych) musi być dokładnie opisany z uwzględnieniem jego charakterystycznych cech oraz wykonaniem zdjęć. Opisanie dowodu musi być zrobione w taki sposób aby nie było wątpliwości co do jego pochodzenia i konfiguracji. Po udokumentowaniu dowodu należy go zaplombować.
- Dowód elektroniczny należy zachować w stanie z chwili zabezpieczenia (czyli jeśli np. telefon został zabezpieczony jako włączony to w takim stanie ma on pozostać). W protokole trzeba odnotować dokładną datę i czas zabezpieczenia sprzętu.
- W przypadku, gdy istnieje konieczność zatrzymania danych z pominięciem sprzętu komputerowego należy wykonać kopię binarną czyli kopię utworzoną na zasadzie równości z oryginałem.

BERNADETTA
STACHURA – TERLECKA

Dobre praktyki

- Kolejnym krokiem na trasie naszych dobrych praktyk zajmuje weryfikacja integralności materiału dowodowego. W zasadzie możemy osiągnąć go poprzez wyliczenie sumy kontrolnej nośnika.
- Jak już wielokrotnie wcześniej wspominałam wszystkie badania, analizy itp. muszą być przeprowadzane w miarę możliwości na kopii binarnej danych a nie na oryginalnym dowodzie.
- Jeśli jednak zajdzie konieczność prowadzenia badań na oryginalnym nośniku wszystkie operacje należy przeprowadzać z wykorzystaniem urządzenia uniemożliwiającego wprowadzenie zmian w dowodzie elektronicznym tzw. brokerów.

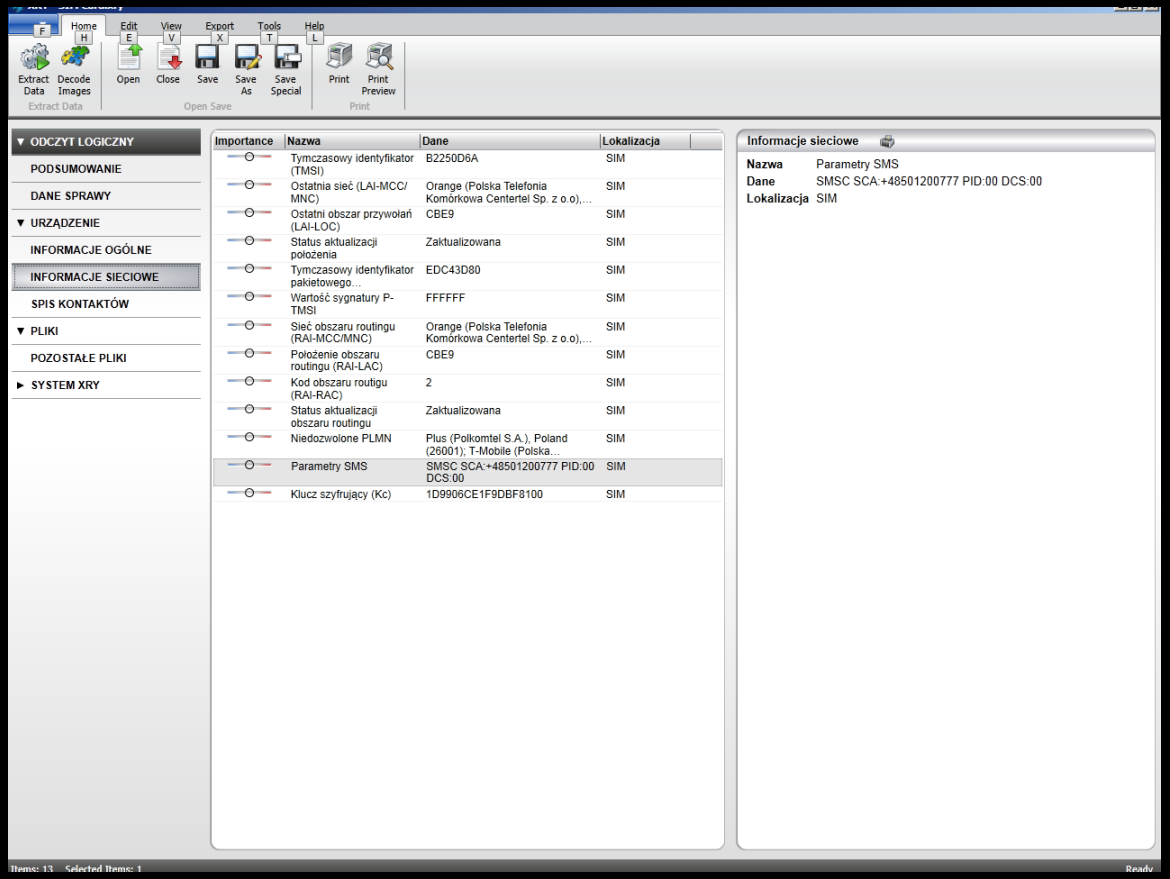
BERNADETTA
STACHURA – TERLECKA

PRZYKŁAD DZIAŁANIA OPROGRAMOWANIA DO ANALIZY URZĄDZEŃ MOBILNYCH XRY

BERNADETTA STACHURA – TERLECKA

Analiza urządzeń mobilnych – karta SIM

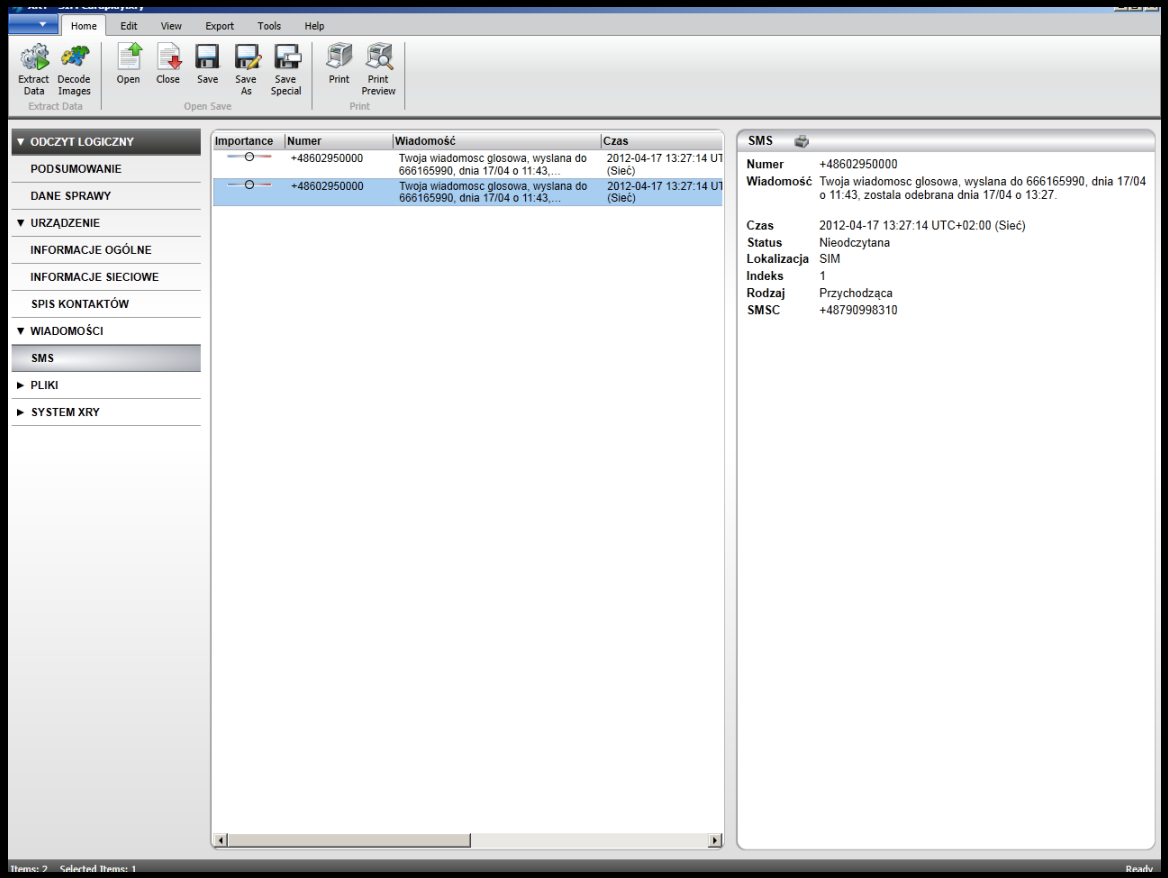
Numer centrum smsów SMSC SCA dla telefonu w sieci Orange



BERNADETTA STACHURA - TERLECKA

Sprawdzenie czy smses jest fałszywy

W sieci istnieją bramki sms umożliwiające przesłanie smsa którego nadawcą jest podany przez nas numer. Dzięki informacji o numerze centrum sms możemy podejrzewać,że sms został / nie został faktycznie wysłany przez nadawcę.



BERNADETTA STACHURA - TERLECKA