BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Wykład 8

8. Wybrane zagadnienia informatyki śledczej

1. Definicja informatyki śledczej
2. Cel dla którego powstała informatyka śledcza
3. Rola informatyki śledczej
4. Zadania informatyki śledczej
5. Narzędzia stosowane w informatyce śledczej
   1. Dane ulotne
   2. Software
   3. Chroń swoją prywatność (?) - antysoftware
   4. Hardware
6. Dowody cyfrowe

8.1. Definicja

– **Informatyka śledcza** (Computer Forensics) jest gałęzią nauk sądowych, której celem jest dostarczanie cyfrowych środków dowodowych popełnionych przestępstw lub nadużyć (1).

źródło - Wikipedia

8.2. Cele dla których powstała

1. **zbieranie, odzyskiwanie, analiza oraz prezentacja, w formie specjalistycznego raportu, danych cyfrowych znajdujących się na różnego rodzaju nośnikach** (dyski twarde komputerów, dyskietki, płyty CD, pamięci przenośne, serwery, telefony komórkowe itp.).

źródło - Wikipedia

8.2. Cele dla których powstała

2. **odtworzenie kolejności działań na komputerze lub innym urządzeniu elektronicznym użytkownika w czasie** (kto to zrobił? co zrobił? gdzie? kiedy to zrobił? jak to zrobił?), **na podstawie informacji niedostępnych (**lub niewidocznych**) dla użytkowników i administratorów systemu.**

5

8.2. Cele dla których powstała

3. **zabezpieczenie i złożenie wszystkich tych fragmentów informacji w jedną całość w sposób spełniający kryteria dowodowe i zgodnie z obowiązującymi w danym kraju regulacjami prawnymi, tak by mogły spełniać rolę dowodu.**

6

8.3. Rola informatyki śledczej

1. **informacyjna** – (wskazówki pomocne w prowadzeniu dochodzenia) - dostarcza wskazówki i ślady, które umożliwiają dalsze zgłębianie poszczególnych zagadnień lub rozszerzenie dochodzenia o nowe wątki

7

8.3. Rola informatyki śledczej

2. **dowodowa** – dostarcza dowody popełniania określonych czynów - umożliwia niepodważalne dowiedzenie popełnienia określonych czynów lub posiadania określonych danych i/lub informacji.

8

8.4. Zadania informatyki śledczej

1. **ustalanie przedmiotu poszukiwania i zakresu analizy dowodów elektronicznych,**
2. **zbieranie, odzyskiwanie i właściwe zabezpieczenie kopii danych,**

9

8.4. Zadania informatyki śledczej

3. **analiza śladów elektronicznych,**
4. **sporządzenie raportu dotyczącego analizowanych danych – prezentacja danych cyfrowych znajdujących się na różnego rodzaju nośnikach** (dyski twarde komputerów, dyskietki, płyty, pamięci przenośne, serwery, telefony komórkowe itp.).

10

8.5. Narzędzia stosowane w informatyce śledczej

Sprzęt komputerowy:

a) blokery, które pozwalają na bezpieczny odczyt nośników danych zawierających ewentualny materiał dowodowy (read only),
b) urządzenia do analizy i zbierania danych z nośników,
c) wyspecjalizowane zestawy przeznaczone do prowadzenia śledztw „w terenie”.

11

8.5. Narzędzia stosowane w informatyce śledczej

Programy narzędziowe do :

a) zabezpieczania danych ,
b) analizy danych,
c) zobrazowania danych.

12

8.5. Narzędzia stosowane w informatyce śledczej

Dane ulotne - dane zawarte w pamięci działającego urządzenia, które są nieodwracalnie tracone w momencie jego wyłączenia.

13

8.5.1. Przykłady danych ulotnych

- **aktualna data i czas,**
- **zawartość pamięci ulotnej** (pamięć RAM i pliki swap),
- **połączenia sieciowe** (otwarte porty TCP lub UDP, NetBIOS, informacja o komputerach znajdujących się w tej samej sieci, pakiety sieciowe),
- **zalogowani użytkownicy, konta użytkowników,**
- **zawartość schowka systemowego,**

14

8.5.1. Przykłady danych ulotnych

- **działające procesy i usługi,**
- **zaplanowane zadania,**
- **otwarte pliki i rejestry,**
- **dane z autouzupełnienia** (np. z przeglądarek, hasła, itp.),
- **zrzut ekranu,**
- **skasowane dane**

15

8.5.1. Zbieranie danych ulotnych - o czym należy pamiętać

- **o wykonaniu obliczenia sumy kontrolnej MD5 wszystkich plików znajdujących się na badanych/analizowanych nośnikach.**
- **jeśli komputer jest wyłączony to pod żadnym pozorem nie wolno go włączać gdyż w ten sposób naruszymy integralność znajdujących się tam danych, logów itp.**

16

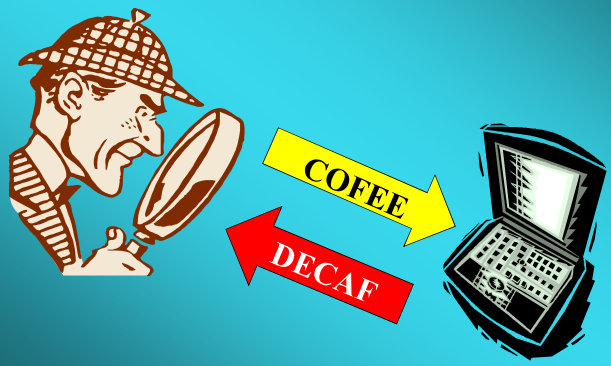
8.5.2. Przykładowe narzędzia do zabezpieczania danych (forensic tools)

- **COFEE - Computer Online Forensic Evidence Extractor** (5),
- **F.I.S.T.** (Live Forensic and Incident Response Toolkit)
- wiele innych…

(5) - http://www.microsoft.com/industry/government/solutions/cofee/default.aspx

17

8.5.3. Antynarzędzia (anti-forensic tools)



18

8.5.3. Antynarzędzia (anti-forensic tools)

W przypadku ujawnienia przez DECAF próby uruchomienia COFEE, program:
− wyłącza obsługę dysków USB,
− generuje dziesiątki przypadkowych adresów MAC w taki sposób aby utrudnić pracę analizującym komputer,
− zamyka uruchomione procesy,
− blokuje połączenia i urządzenia sieciowe,
− blokuje porty USB i stację dysków,
− blokuje napędy CD / DVD oraz port drukarki,
− usuwa pliki i foldery wskazane i zdefiniowane w opcjach programu,

19

8.5.3. Antynarzędzia (anti-forensic tools)

W przypadku ujawnienia przez DECAF próby uruchomienia COFEE program:
− usuwa klientów sieci P2P i foldery, do których zapisywały one pobierane z sieci dane,
− powoduje wyczyszczenie plików cookies, historii przeglądanych stron oraz danych zapamiętanych przez przeglądarkę,
− uniemożliwia wykonanie zrzutu ekranowego,
− powoduje wyłączenie komputera.

20

8.5.4. Przykład narzędzia mobilnego do zabezpieczania danych (forensic tools)

21

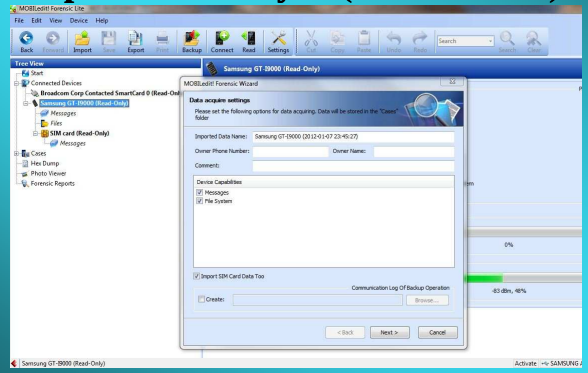
8.5.4. Przykład narzędzia mobilnego do zabezpieczania danych (forensic tools)

22

8.5.4. Przykład narzędzia mobilnego do zabezpieczania danych (forensic tools)

23

8.5.4. Przykład narzędzia mobilnego do zabezpieczania danych (forensic tools)



24

8.6.1. Dowód cyfrowy - definicja

- sprzęt komputerowy, oprogramowanie lub dane, które mogą być użyte w celu udowodnienia dokonania przestępstwa elektronicznego i odpowiedzieć na jedno lub wiele z pytań: kto, co, kiedy, gdzie, dlaczego oraz w jaki sposób?

25

8.6.1. Dowód cyfrowy - definicja

- **informacja zapisana lub transmitowana w formie elektronicznej, mająca znaczenie w postępowaniu sądowym**

26

8.6.2. Dowód cyfrowy – inne nazwy

- **„dowód elektroniczny”** (electronic evidence),
- **„dowód komputerowy”** (computer evidence),
- **„dowód wygenerowany komputerowo”** (computer – generated evidence),
- **„dowód utworzony na skutek działania komputera”** (computer – based evidence),
- **„dowód pochodzący z komputera”** (computer – derived evidence),
- **„dowód IT”** (IT evidence)

27

8.6.3. Dowód cyfrowy – warunki

Dowód cyfrowy, który ma być użyty w procesie sądowym musi:

- **być istotny**
- **być kompletny**
- **być prawdziwy**
- **być niepodważalny**
- **być przekonywujący**
- **być zdobyty zgodnie z prawem**

28

8.6.4. Klasyfikacja dowodów cyfrowych

1. **dane pochodzące z podsłuchu:**
   a) **w postaci treści przesyłanej informacji,**
   b) **w postaci danych adresowych odbiorcy i nadawcy informacji,**
2. **dane przechowywane w systemie komputerowym lub archiwizowane na nośnikach informacji:**
   a) **w postaci dokumentów elektronicznych i poczty elektronicznej,**
   b) **w postaci danych transakcyjnych,**
   c) **w formie rejestru operacji dokonanych przez użytkowników systemu**

Adamski A. – Prawo karne komputerowe, Wa-wa 2000

8.6.4. Dowód cyfrowy – klasyfikacja 2

- **1. ze względu na sposób uzyskania:**
  - **pochodzące z podsłuchu,**
  - **przechowywane w systemie lub na elektronicznych nośnikach informacji,**
- **2. ze względu na rodzaj danych:**
  - **zawierające tekst,**
  - **zawierające zapisy obrazu,**
  - **zawierające zapisy dźwięku,**
- **3. ze względu na rodzaj zapisu:**
  - **analogowe,**
  - **cyfrowe,**
- **4. ze względu na sposób powstania zapisu przy dowodach cyfrowych:**
  - **cyfrowe sensu stricte,**
  - **zdigitalizowane,**
- **5. ze względu na źródło dowodowe:**
  - **właściwe dowody rzeczowe,**
  - **dokumenty,**
- **6. ze względu na sposób wykorzystania:**
  - **samoistne,**
  - **niesamoistne**

Lach A. Dowody elektroniczne w procesie karnym s. 36

8.6.5. Rola dowodów cyfrowych

Główną rolą jest ich funkcja jako przedmiotów:

- służących do popełnienia przestępstwa,
- pochodzących z przestępstwa,
- które mogły zachować cechy przestępstwa,
- które mogą służyć jako środek dowodowy do wykrycia sprawcy czynu lub ustalenia przyczyn i okoliczności przestępstwa,
- których posiadanie bez zezwolenia jest zabronione.

8.6.6. Dopuszczalność dowodów cyfrowych

W polskim ustawodawstwie, by zostać dopuszczonym w sądzie, dowód elektroniczny musi spełniać poniższe wymogi:

- **musi być uznany za wiarygodny,**
- **musi być istotny, czyli udowadniać fakt związany ze sprawą,**
- **musi być materialny, czyli dotyczyć kwestii związanych ze sprawą.**

Lach A. Dowody elektroniczne w procesie karnym

8.6.6. Niszczenie dowodów cyfrowych – techniki anty-forensic

celowe działania sprawców polegające na utrudnieniu, lub uniemożliwieniu przeprowadzenia badania sprzętu lub oprogramowania komputerowego

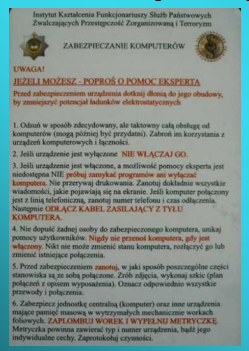
8.6.6. Niszczenie dowodów cyfrowych – techniki anty-forensic

- zabezpieczenie przed uruchomieniem w trybie debbugowania (uzyskania czytelności kodu jakim napisany został analizowany program),
- ukrywanie danych,
- szyfrowanie danych,
- steganografia,
- odmowa uruchomienia procedur przy zastosowaniu maszyny wirtualnej (praca na obrazie dysku),
- rozproszenie sieciowe lub systemowe,
- umyślne kasowanie danych,
- niszczenie nośników danych,
- zmiana zawartości plików poprzez nadpisywanie danych nowymi danymi,
- manipulacja meta danymi plików,
- wykorzystanie maszyn, dysków i folderów wirtualnych,
- używanie sprzętowych systemów typu „recovery card”,
- zabezpieczenia przed analizą narzędziami informatyki śledczej

8.6.7. Problemy przy zabezpieczaniu dowodów cyfrowych

- brak właściwego przygotowania technicznego i taktycznego organów ścigania do zabezpieczenia elektronicznych śladów przestępstw
- brak aktywnej współpracy pomiędzy Policją, prokuraturą, sądami, biegłymi oraz pokrzywdzonymi,
- niewystarczające zaplecze techniczne oraz brak dostatecznej wiedzy, a co za tym idzie, niechęć do prowadzenia skomplikowanych postępowań z zakresu cyberprzestępczości
- w konsekwencji - spadek wykrywalności przestępstw

8.6.7. Problemy przy zabezpieczaniu dowodów cyfrowych - instrukcja



Instytut Kształcenia Funkcjonariuszy Służb Państwowych Zwalczających Przestępczość Zorganizowaną i Terroryzm

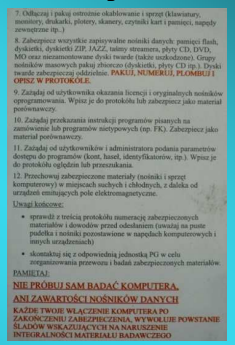
ZABEZPIECZANIE KOMPUTERÓW

UWAGA!

JEŻELI MOŻESZ - POPROŚ O POMOC EKSPERTA

Przed zabezpieczeniem urządzenia dotknij dłonią do jego obudowy, by zmniejszyć potencjał ładunków elektrostatycznych

1. Odsuń w sposób zdecydowany, ale taktowny całą obsługę od komputerów (mogą później być przydatni). Zabroń im korzystania z urządzeń komputerowych i łączności.
2. Jeśli urządzenie jest wyłączone NIE WŁĄCZAJ GO.
3. Jeśli urządzenie jest włączone, a możliwość pomocy eksperta jest niedostępna NIE próbuj zamykać programów ani wyłączać komputera. Nie przerywaj drukowania. Zanotuj dokładnie wszystkie wiadomości, jakie pojawiają się na ekranie. Jeśli komputer połączony jest z linią telefoniczną, zanotuj numer telefonu i czas odłączenia. Następnie ODŁĄCZ KABEL ZASILAJĄCY Z TYŁU KOMPUTERA.
4. Nie dopuść żadnej osoby do zabezpieczonego komputera, unikaj pomocy użytkowników. Nigdy nie przenoś komputera, gdy jest włączony. Nikt nie może zmienić stanu komputera, rozłączyć go lub zmienić istniejące połączenia.
5. Przed zabezpieczeniem zanotuj, w jaki sposób poszczególne części stanowiska są ze sobą połączone. Zrób zdjęcia, wykonaj szkic (plan połączeń i spisem wyposażenia). Oznacz odpowiednio wszystkie przewody i połączenia.
6. Zabezpiecz jednostkę centralną (komputer) oraz inne urządzenia mając pamięć masową w wyżrzymałych mechanicznie workach foliowych. ZAPLOMBUJ WOREK I WYPEŁNIJ METRYCZKĘ. Metryczka powinna zawierać typ i numer urządzenia, bądź jego indywidualne cechy. Zaprotokołuj czynności.



7. Odłączaj i pakuj ostrożnie okablowanie i sprzęt (klawiatury, monitory, drukarki, plotery, skanery, czytniki kart i pamięci, napędy zewnętrzne itp..)
8. Zabezpiecz wszystkie zapisywalne nośniki danych: pamięci flash, dyskietki, dyskietki ZIP, JAZZ, taśmy streamera, płyty CD, DVD, MO oraz niezamontowane dyski twarde (także uszkodzone). Grupy nośników masowych pakuj zbiorczo (dyskietki, płyty CD itp.). Dyski twarde zabezpieczaj oddzielnie. PAKUJ, NUMERUJ, PLOMBUJ I OPISZ W PROTOKOLE.
9. Zażądaj od użytkownika okazania licencji i oryginalnych nośników oprogramowania. Wpisz je do protokołu lub zabezpiecz jako materiał porównawczy.
10. Zażądaj przekazania instrukcji programów pisanych na zamówienie lub programów nietypowych (np. FK). Zabezpiecz jako materiał porównawczy.
11. Zażądaj od użytkowników i administratora podania parametrów dostępu do programów (konf, hasel, identyfikatorów, itp.). Wpisz je do protokołu oględzin lub przeszukania.
12. Przechowuj zabezpieczone materiały (nośniki i sprzęt komputerowy) w miejscach suchych i chłodnych, z dalska od urządzeń emitujących pole elektromagnetyczne.

Uwagi końcowe:

- sprawdź z treścią protokołu numerację zabezpieczonych materiałów i dowodów przed odebraniem (uważaj na puste pudełka i nośniki pozostawione w napędach komputerowych i innych urządzeniach)
- skontaktuj się z odpowiednią jednostką PG w celu zorganizowania przewozu i badań zabezpieczonych materiałów.

PAMIĘTAJ:

NIE PRÓBUJ SAM BADAĆ KOMPUTERA,

ANI ZAWARTOŚCI NOŚNIKÓW DANYCH

KAŻDE TWOJE WŁĄCZENIE KOMPUTERA PO ZAKOŃCZENIU ZABEZPIECZENIA, WYWOŁUJE POWSTANIE ŚLADÓW WSKAZUJĄCYCH NA NARUSZENIE INTEGRALNOŚCI MATERIAŁU BADAWCZEGO

http://www.arimr.gov.pl/uploads/media/Zalacznik_nr_6_do_wzoru_umowy_01.pdf s.99

Czy są …

jakieś pytania ?

37

DODATEK

Co jest dla Ciebie informacją najbardziej wrażliwą ?