

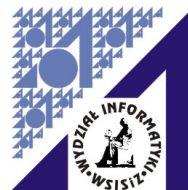
**WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ
I ZARZĄDZANIA**

pod auspicjami Polskiej Akademii Nauk



WYDZIAŁ INFORMATYKI

STUDIA II STOPNIA
(MAGISTERSKIE)



PRACA DYPLOMOWA

Krzysztof Bińkowski

**ANALIZA POWŁAMANIOWA
W SYSTEMACH MICROSOFT
WINDOWS**

Praca wykonana pod kierunkiem:

dr inż. Bożeny Łopuch

WARSZAWA, 2009 r.

Autor: **Krzysztof Bińkowski**

Tytuł: **ANALIZA POWŁAMANIOWA W SYSTEMACH MICROSOFT
WINDOWS**

Rok akademicki: **2008/2009**

Dziekan Wydziału: **dr inż. Jarosław Sikorski**

Specjalność: **Teleinformatyka**

Opiekun pracy: **dr inż. Bożena Łopuch**

Niniejszą pracę dedykuję mojej towarzyszce życia - ukochanej żonie Eli oraz córce Karolinie i synkowi Wiktorkowi, dziękując za ich wsparcie i pomoc, chcę w ten sposób wynagrodzić im mój czas spędzony przy komputerze który im zabrałem ...

Kontakt z autorem: **Krzysztof.Binkowski@gmail.com**

WSTĘP	5
1. INFORMATYKA ŚLEDZCZA	6
1.1 Dowód elektroniczny	7
1.2 Łańcuch dowodowy	7
1.3 Uwarunkowania prawne związane z informatyką śledczą	9
2. MODEL ANALIZY INFORMATYKI ŚLEDCZEJ	12
2.1 Ocena sytuacji	12
2.1.1 Uzyskanie formalnego upoważnienia do przeprowadzenia śledztwa	12
2.1.2 Zapoznanie się z obowiązującą polityką bezpieczeństwa.....	13
i procedurami.....	13
2.1.3 Wyznaczenie członków zespołu śledczego.....	14
2.1.4 Przeprowadzenie szczegółowej oceny sytuacji.....	14
2.2 Pozyskiwanie danych.....	15
2.2.1 Przygotowanie zestawu narzędzi do przeprowadzenia śledztwa	15
2.2.2 Zbieranie danych.....	16
2.2.3 Przechowywanie i magazynowanie zgromadzonych danych	17
2.3 Analiza danych.....	18
2.3.1 Analiza danych sieciowych.....	18
2.3.2 Analiza danych znajdujących się na komputerze.....	19
2.3.3 Analiza nośników danych	19
2.4 Raport ze śledztwa	20
2.4.1 Zgromadzenie i uporządkowanie pozyskanych informacji.....	21
2.4.2 Utworzenie końcowego raportu	21
3. ZBIERANIE DANYCH	23
3.1 Przygotowanie do zbierania danych	23
3.2 Dane ulotne	26
3.3 Proces zbierania danych ulotnych.....	26
3.3.1 Zbieranie informacji na temat bieżącej konfiguracji i stanów procesów	26
3.3.2 Zbieranie informacji na temat stanu połączeń sieciowych	32
3.4 Dane nieulotne	34
3.5 Proces zbierania danych nieulotnych.....	35
4. ANALIZA ZGROMADZONYCH DANYCH.....	40

4.1	Typy i rodzaje szukanych danych.....	40
4.2	Charakterystyczne miejsca do poszukiwania danych	41
4.3	Pliki skompresowane ZIP,RAR,CAB, etc.	45
4.4	Poczta elektroniczna pliki charakterystyczne	45
4.5	Alternatywne strumienie danych	46
4.6	Pliki graficzne i steganografia.....	48
4.7	Rootkity.....	49
4.8	Rejestr systemowy	51
4.9	Odzyskiwanie skasowanych plików	53
4.10	Użytkownicy i hasła	56
4.11	Dane zaszyfrowane	56
4.12	Logi systemowe i ich analiza	57
5.	PRZEGLĄD NARZĘDZI STOSOWANYCH.....	62
	W INFORMATYCE ŚLEDZCZEJ	62
5.1	Przeгляд darmowych zestawów narzędzi	62
5.2	Przeгляд komercyjnych zestawów narzędzi	65
6.	ANALIZA PRZYPADKU.....	68
6.1	Scenariusz	68
6.2	Opis przygotowanego środowiska testowego.....	69
6.3	Analiza	69
6.3.1	Oszacowanie sytuacji	70
6.3.2	Pozyskiwanie danych	70
6.3.3	Analiza zgromadzonych danych	71
6.3.4	Przygotowanie raportu:	75
	PODSUMOWANIE	77
	BIBLIOGRAFIA:.....	78
	Załącznik 1- Wzór łańcucha dowodowego	80
	Załącznik 2 – Zawartość płyt dołączonych do pracy	81
	Załącznik 3 - Raport końcowy.....	82

WSTĘP

Analiza powłamaniowa jest jednym z elementów tzw. informatyki śledczej (*ang. computer forensics*). Zajmuje się pozyskiwaniem i poszukiwaniem śladów pozostawionych w skompromitowanych systemach komputerowych. Jej celem jest gromadzenie dowodów do postępowania sądowego lub po prostu analiza informacji, które pozwolą odtworzyć metodologię ataku zastosowaną przez cyberprzestępców. Potrzebne informacje są w większości przypadków przechowywane w systemie, ale kluczowym problemem jest ich wydobycie.

Celem pracy jest przedstawienie wzorcowego modelu analizy informatyki śledczej wraz z praktycznymi przykładami stosowanych technik i narzędzi (darmowych i komercyjnych), które mogą być wykorzystane do analizy pozostawionych śladów działalności przestępczej w systemach Windows. Praca ma odpowiedzieć na pytania jak szukać śladów włamania (często zatartych) oraz jak przygotować znalezione informacje jako dowody popełnionego wykroczenia lub przestępstwa komputerowego.

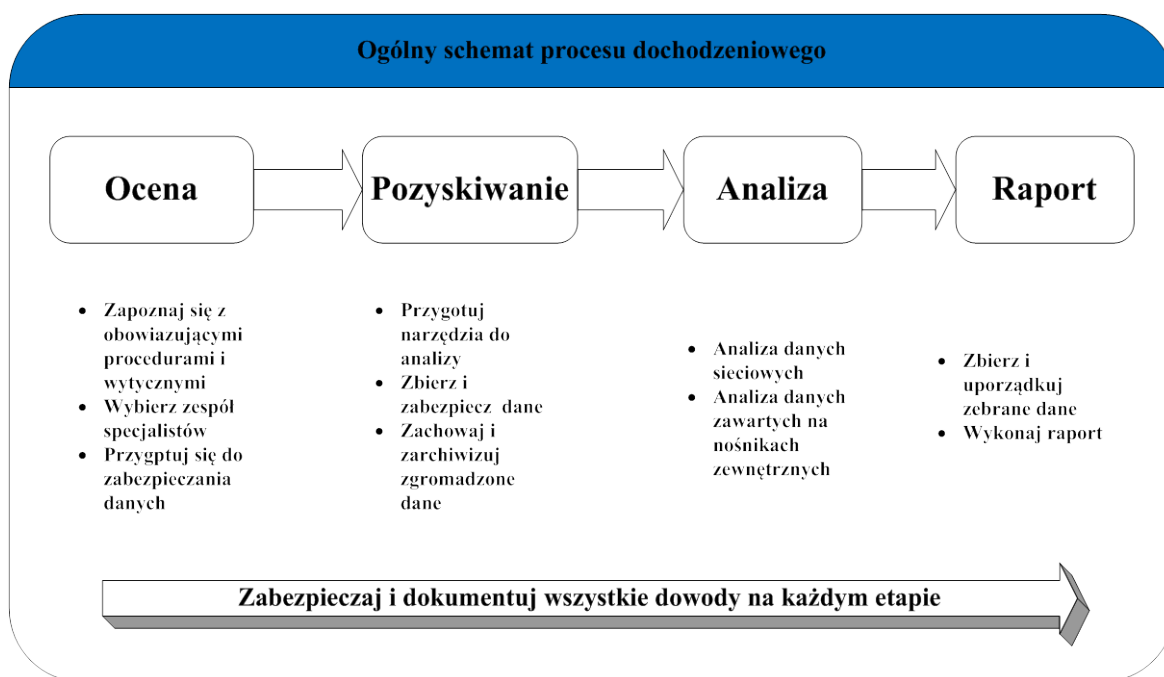
Jednym z głównych aspektów informatyki śledczej świadczących o powodzeniu przyszłej analizy jest prawidłowe pozyskiwanie danych. Zbieranie danych powinno być wykonane z należytą starannością i w odpowiedniej kolejności, ponieważ najmniejszy błąd może skutkować zatarciem informacji i śladów w badanym systemie. W pracy zostaną zaprezentowane sposoby pozyskiwania danych z uwagi na ich ulotność. Przedstawione zostaną również sposoby ukrywania informacji w plikach oraz sposoby przeszukiwania takich plików. Jednym z miejsc ukrywania danych może być sam system plików. W pracy przedstawione zostaną sposoby wykorzystywania właściwości systemu NTFS do ukrycia informacji.

Praktyczny aspekt zastosowania informatyki śledczej zostanie pokazany na przykładzie analizy rzeczywistego przypadku. W toku badań zostanie przeprowadzona własna wzorcowa analiza na komputerze z systemem Microsoft Windows XP z wykorzystaniem opisanych w pracy technik i narzędzi. Analiza zaprezentuje sposób zabezpieczenia danych z dysku trwałego, który może posłużyć jako dowód elektroniczny. Wynikiem przeprowadzonego badania będzie raport zawierający znalezione dowody świadczące o popełnieniu wykroczenia przeciwko ochronie informacji.

1. INFORMATYKA ŚLEDICZA

Informatyka śledcza¹ (*ang. Computer Forensics*) jest to dziedzina wiedzy, która zajmuje się dostarczaniem elektronicznych dowodów przestępstwa. Jako efekt pracy końcowej specjalistów zajmujących się informatyką śledczą powstaje raport lub analiza specjalistyczna stanowiąca materiał dowodowy w prowadzonym dochodzeniu.

Sam proces analizy śledczej², jest to zespół określonych czynności wykonanych w określonych warunkach i odpowiednio udokumentowanych, służących do dostarczenia organom ścigania lub komórkom dochodzeniowym wiarygodnych danych o wartości dowodowej. Proces analizy informatyki śledczej możemy podzielić na cztery etapy (Rys. 1.1): zaplanowanie działań, zbieranie informacji, przeprowadzenie analizy danych i wykonanie raportu. Etapy te są dokładnie omówione w dalszej części pracy.



Rysunek 1.1 - Ogólny schemat procesu dochodzeniowego stosowanego w informatyce śledczej. (źródło - [MICROSOFT1], strona 1)

¹ Informatyka śledcza (*ang. computer forensic*) pełną definicję znajdziemy: w języku polskim - http://pl.wikipedia.org/wiki/Informatyka_%C5%9Bledcza oraz obszerniejsza definicja w języku angielskim - http://en.wikipedia.org/wiki/Computer_forensics

² Definicja wg Wikipedii - Informatyka śledcza (*ang. computer forensic*) - http://pl.wikipedia.org/wiki/Informatyka_%C5%9Bledcza

1.1 Dowód elektroniczny

Dowodem elektronicznym (*ang. electronic evidence*)³ nazywamy jakikolwiek sprzęt komputerowy, oprogramowanie lub dane, które możemy użyć, aby udowodnić dokonanie przestępstwa komputerowego i odpowiedzieć na jedno z pytań: kto, co, kiedy, gdzie, dlaczego oraz w jaki sposób. W chwili obecnej najczęstszym dowodem fizycznym jest dysk twardy, komórka, palmtop czy wszelkie nośniki takie jak dyskietki, płyty CD/DVD, pamięci flash, karty pamięci, taśmy lub inne nośniki magnetyczne.

Elementem potwierdzającym wiarygodność działań związanych z dowodami elektronicznymi jest funkcja skrótu (*ang. hash*), – która niemal na każdym kroku analizy jest wykorzystywana, a szerzej zostanie omówiona w dalszych rozdziałach. Operacja ta kontroluje i sprawdza dany plik lub cały dysk pod kątem modyfikacji i ingerencji w dane oraz pozwala nam określić czy nie popełniliśmy błędu przy analizie danego nośnika.

Dowód, który będzie użyty w procesie sądowym powinien być:

- kompletny,
- prawdziwy,
- niepodważalny,
- przekonywujący,
- zdobyty zgodnie z prawem.

Spełnienie wszystkich warunków będzie świadczyło o wiarygodności dowodu i taki dowód nie zostanie odrzucony w sądzie podczas procesu. Należy pamiętać o tym podczas procesu zbierania dowodów elektronicznych.

1.2 Łańcuch dowodowy

Łańcuchem dowodowym (*ang. chain of custody*) określamy cały proces od momentu pozyskania dowodu, aż do przedstawienia go w sądzie⁴. Łańcuch ten jest bardzo obszerną dokumentacją, opisującą krok po kroku wszystkie czynności wykonywane w stosunku do dowodu elektronicznego, od pozyskania dowodu, poprzez jego transport, zgromadzenie zawartych w nim informacji i dokonanie analizy, po miejsce i sposób przechowywania. Dokument taki jest bardzo istotny, musi być prowadzony w sposób chronologiczny i nie może zawierać żadnych luk w zapisie.

³ Definicja według [CF JUMPSTART]

⁴ Definicja według [CF JUMPSTART]

Początkiem każdego łańcucha dowodowego jest protokół z zabezpieczenia dowodu. W dokumencie tym powinny być odnotowane dzień, godzina i miejsce zabezpieczenia, a także suma kontrolna, która jest unikalna dla każdego nośnika (np. dla danego dysku twardego, płyty CD/DVD). Siłą sumy kontrolnej jest to, że można ją wyliczyć ponownie w dowolnym momencie i wykazać, że dowód nie został zmodyfikowany lub zmieniony. Protokół musi podpisać komisja, która składa się z osób dokonujących analizy a także, jeśli istnieje taka możliwość, wskazany jest podpis właściciela lub adwokata.

Każdy kolejny dostęp do dowodu powinien być opisany ze szczególną starannością i musi zawierać przynajmniej:

- Datę i czas działania;
- Typ akcji (wstępna ewidencja, zmiana miejsca przetrzymywania, pobranie dowodu do analizy, zwrot dowodu);
- Imię i nazwisko osób mających kontakt z dowodem;
- Opis użytego komputera (model, marka, numer seryjny, lokalizacja, inne cechy identyfikacyjne, specyficzne ustawienia BIOSu);
- Szczegółowy opis dysku (producent, model, parametry dysku, ustawienie zworek, sposób podłączenia do komputera –master/slave);
- Procedura postępowania z dyskiem (przygotowanie miejsca pracy, środki bezpieczeństwa antystatycznego, opis działań krok po kroku, spis wszystkich czynności (informacja o pliku, katalogu, dysku i jego suma kontrolna);
- Sumaryczny opis działania (wykorzystana procedura, opis użytych narzędzi, opis każdego działania i jego wyniki);
- Powód działania;
- Notatki (komentarze, uwagi, a także dodatkowe informacje, ujawnione podczas procesu);

Łańcuch dowodowy jest dokumentem, który powinien być tworzony z należytą starannością i chroniony pod szczególnym nadzorem. Wiarygodność tego dokumentu może zaważyć, na jakości dowodu elektronicznego użytego w sprawie. Przykładowy dokument został przedstawiony w załączniku numer 1.

1.3 Uwarunkowania prawne związane z informatyką śledczą

Przestępstwa popełnione przeciwko ochronie informacji uwzględniające przestępczość komputerową znajdują się już w kodeksie karnym i zawarte są w artykułach 267-269 a także 287 Kodeksu karnego⁵, przytoczymy je w celu zapoznania się z nimi oraz przewidzianymi karami za te czyny w polskim prawie:

Art. 267.

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Art. 268.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

⁵ - Kodeks Karny z dnia 6 czerwca 1997, źródło Dziennik Ustaw 1997 nr 88 poz. 557 – źródło [http://isip.sejm.gov.pl/PRAWO.nsf/4326b1a242fc14fd412563d20069fee3/dcffcc6c7c83f965c1256657004e231c/\\$FILE/D19970553Lj.pdf](http://isip.sejm.gov.pl/PRAWO.nsf/4326b1a242fc14fd412563d20069fee3/dcffcc6c7c83f965c1256657004e231c/$FILE/D19970553Lj.pdf) (stan prawny na dzień 2009-01-02)

Art. 269.

§ 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a.

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b.

§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269

§ 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Art. 287.

§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Artykuł 287 kodeksu karnego określa przestępstwa komputerowe, np. wykasowanie danych z elektronicznych nośników informacji, takich jak dyski twarde swojego pracodawcy, jako przestępstwo komputerowe, które zagrożone jest karą pozbawienia wolności od 3 miesięcy do 5 lat, a w przypadku mniejszej wagi kodeks przewiduje karę w postaci grzywny, ograniczenia wolności lub pozbawienia wolności do 1 roku.

Informatyka śledcza jest narzędziem wspomagającym pracodawców w obronie przed nieuczciwymi pracownikami dokonującymi ujawnienia, sprzedaży lub celowego usunięcia poufnych danych. Działanie to możemy określić mianem naruszenia zasad obowiązującej umowy o pracę zawieranej pomiędzy pracodawcą a pracownikiem.

Zgodnie z artykułem 52 par. 1 pkt. 1 kodeksu pracy⁶ ujawnienie, kradzież lub wykasowanie poufnych danych przez pracownika może stanowić podstawę do rozwiązania umowy o pracę przez pracodawcę bez wypowiedzenia i w przytoczonym artykule stanowią przykład „ciężkiego naruszenia przez pracownika podstawowych obowiązków pracowniczych”.

Ujawnienie, przekazanie lub wykorzystanie przez pracownika informacji stanowiących tajemnicę przedsiębiorstwa stanowi czyn nieuczciwej konkurencji zgodnie z art. 11 ustawy o zwalczaniu nieuczciwej konkurencji⁷. Ponadto art. 23 wspomnianej ustawy stanowi:

„Kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.”

Wnioskując z przytoczonych aspektów prawnych, możemy powiedzieć, że działania pracownika na szkodę pracodawcy, które mogą zostać ujawnione dzięki informatyce śledczej, w polskim prawie są obecne i pracownicy nie mogą czuć się bezkarnie manipulując powierzonymi im poufnymi danymi. Przytoczne przykłady pokazują jak pomocne może okazać się śledztwo z zakresu informatyki śledczej przeciwko podejrzanym pracownikom, działającym na szkodę swojego pracodawcy.

⁶ Kodeks pracy - Dz.U. 1974 Nr 24 poz. 141 , USTAWA z dnia 26 czerwca 1974 r. ,
<http://isip.sejm.gov.pl/servlet/Search?todo=file&id=WDU19740240141&type=3&name=D19740141Lj.pdf>
(stan na dzień 2009-02-02)

⁷ Dz.U. 1993 nr 47 poz. 211, Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.
<http://isip.sejm.gov.pl/servlet/Search?todo=file&id=WDU19930470211&type=3&name=D19930211Lj.pdf>

2. MODEL ANALIZY INFORMATYKI ŚLEDCZEJ

Model informatyki śledczej (ang. *Computer Investigation Model*) wykorzystywany w pracy zaproponowany został w [MICROSOFT1]. Zgodnie z nim w każdym śledztwie komputerowym możemy wyróżnić cztery główne fazy:

- **Ocena sytuacji** (ang. *Assess*) – faza obejmująca analizę zakresu prac do przeprowadzenia w śledztwie wraz z towarzyszącymi działaniami.
- **Pozyskiwanie danych** (ang. *Acquire*) - faza składająca się z gromadzenia, ochrony i zabezpieczenia oryginalnych fizycznych dowodów.
- **Analiza danych** (ang. *Analyze*) – faza polegająca na badaniu, analizie i zestawieniu zebranych dowodów elektronicznych, jest to proces wspomagający ustalenie i odtworzenie przebiegu zdarzeń.
- **Raport ze śledztwa** (ang. *Report*) – ostatnia faza podsumowująca cały proces w oparciu o zgromadzone i uporządkowane informacje w postaci dokumentu końcowego raportu.

Poniżej przedstawiono szczegółowo poszczególne fazy. Opis sporządzono w oparciu o wytyczne zawarte w [MICROSOFT1].

2.1 Ocena sytuacji

Zadaniem tego etapu jest wykonanie szczegółowej oceny sytuacji, ustalenie zakresu wewnętrznego śledztwa oraz wymaganych zasobów. Etap ten składa się z kilku kroków. Pierwszym krokiem jest uzyskanie formalnego upoważnienia do przeprowadzenia śledztwa. Kolejne kroki to zapoznanie się z obowiązującą polityką bezpieczeństwa, wyznaczenie członków zespołu śledczego, przeprowadzenie szczegółowej oceny sytuacji.

2.1.1 Uzyskanie formalnego upoważnienia do przeprowadzenia śledztwa

W celu przeprowadzenia dochodzenia musimy zastosować się do obowiązujących w danym przedsiębiorstwie procedur i polityk bezpieczeństwa, które opisują szczegółowo działanie w takich sytuacjach. Jeśli takie dokumenty nie istnieją, musimy uzyskać zgodę na rozpoczęcie działań śledczych od naszych zwierzchników, przełożonych lub bezpośrednio od zarządu organizacji, dla której pracujemy lub świadczymy usługi. Po uzyskaniu zgody,

należy oszacować zastałą sytuację i wyznaczyć dalszy przebieg działań. Mogą być tutaj przydatne tzw. najlepsze praktyki⁸ zaproponowane w [MICROSOFT1]:

- Pamiętaj o dokumentowaniu wszystkich wykonywanych kroków związanych ze śledztwem. Dokumentacja ta ostatecznie może posłużyć w sądzie, jako przebieg podjętych działań podczas śledztwa.
- Ustal priorytety działań. Zazwyczaj pierwszym priorytetem jest ochrona organizacji przed ewentualnymi szkodami wyrządzonymi w czasie incydentu, po wyeliminowaniu zagrożenia i ewentualnym przywróceniu usług, kolejnym priorytetem będzie prowadzenie śledztwa.

2.1.2 Zapoznanie się z obowiązującą polityką bezpieczeństwa i procedurami

Kolejnym krokiem, który należy wykonać przed rozpoczęciem śledztwa jest zapoznanie się z obowiązującym prawem, oraz wewnętrznymi procedurami i polityką bezpieczeństwa przedsiębiorstwa.

Najlepsze praktyki [MICROSOFT1] podpowiadają nam działania:

Musimy się upewnić, że posiadamy odpowiednie kompetencje i uprawnienia do przeprowadzenia śledztwa. Musimy sprawdzić czy w przedsiębiorstwie istnieją odpowiednie polityki i procedury chroniące prawo do prywatności pracowników i współpracowników korzystających z zasobów sieciowych. Powinniśmy upewnić się czy istnieją odpowiednie procedury określające okoliczności, w których kontrola i przeszukiwanie sieci wewnętrznej jest dopuszczona. Wiele organizacji określa polityki i procedury zatrudnienia, w których zabraniają używania zasobów firmowych do prywatnych celów i zastrzegają sobie prawo do kontrolowania, monitorowania i przeszukiwania zasobów, takich jak poczta elektroniczna, zasoby sieciowe i plikowe lub telefon, mogących zawierać poufne, prywatne dane pracowników. Jeśli nie jesteśmy pewni, czy posiadamy odpowiednie upoważnienie, powinniśmy skontaktować się z zarządem lub radcą prawnym, który pomoże rozwiązać nam nasze wątpliwości.

W szczególności w celu uniknięcia niewłaściwego przeprowadzenia śledztwa powinniśmy skonsultować i poradzić się radcy prawnego lub prawnika w takich kwestiach jak:

⁸Mianem „najlepszych praktyk” określa się procedury i działania, które okazały się w praktyce najbardziej efektywne.

- ujawnienie poufnych danych osobistych, które mogą narazić na szwank daną osobę,
- złamanie lokalnego lub obowiązującego w danym kraju prawa, np. ustawy o ochronie danych osobowych,
- dostęp do danych wrażliwych lub objętych tajemnicą przedsiębiorstwa.

Musimy upewnić się, że zapewniliśmy prywatność i poufność gromadzonych informacji poprzez właściwe przechowywanie danych oraz przechowywanie danych po zamknięciu śledztwa nie dłużej niż przewidują to odpowiednie przepisy prawa lub procedury.

Musimy przechowywać kopie dowodów elektronicznych, materiały dowodowe oraz wydruki, a także łańcuch dowodowy zawierający udokumentowany każdy dowód na wypadek skierowania sprawy na drogę sądową.

2.1.3 Wyznaczenie członków zespołu śledczego

Idealnie byłoby aby zespół został utworzony wcześniej niż nastąpi potrzeba przeprowadzania śledztwa, ale ważniejsze jest trafne dobranie osób posiadających stosowną wiedzę i kwalifikacje.

Najlepsze praktyki [MICROSOFT1] podpowiadają nam działania:

- Wyznaczamy kierownika zespołu, który pokieruje dochodzeniem.
- Wybieramy zespół, przydzielamy i wyjaśniamy każdemu członkowi jego zakres obowiązków i odpowiedzialności. Jeśli dane przedsiębiorstwo nie posiada odpowiednio przeszkolonej kadry w swoich zasobach, należy zaangażować zaufaną zewnętrzną firmę, świadczącą profesjonalne usługi informatyki śledczej,
- Upewniamy się, czy każdy z członków zespołu posiada odpowiednie upoważnienie do prowadzenia wyznaczonych zadań. Ma to szczególne znaczenie, kiedy osoby zewnętrzne, takie jak konsultanci czy eksperci są zaangażowani w śledztwo.

2.1.4 Przeprowadzenie szczegółowej oceny sytuacji

Szczegółowa ocena sytuacji jest potrzebna, aby można było ustawić odpowiednie priorytety i określić zasoby potrzebne do przeprowadzenia dochodzenia. Najlepsze praktyki [MICROSOFT1] podpowiadają nam działania:

- Należy wykorzystać wszystkie dostępne informacje, aby opisać zaistniałą sytuację. Należy określić poziom poufności śledztwa; może ono obejmować na przykład dane klientów, dane finansowe czy tajemnice handlowe przedsiębiorstwa. Ocena ta

przekracza kompetencje działu IT, i powinna być dokonana w porozumieniu z zarządem i prawnikami.

- Należy oszacować koszty incydentu. Należy określić wpływ incydentu na niematerialne koszty naszych zasobów, takie jak reputacja, wizerunek i wiarygodność firmy, relacje z klientami czy morale pracowników.

W celu identyfikacji, analizy i udokumentowania infrastruktury i komputerów, które zostały sytuacją objęte incydem należy [MICROSOFT1]:

- Zidentyfikować segmenty sieci oraz liczbę i typy komputerów, które zostały zaatakowane.
- Uzyskać dokumentację topologii sieci
- Określić zewnętrzne urządzenia pamięciowe (takie jak pamięć USB, karty flash, płyty CD/DVD, taśmy magnetyczne, czy zewnętrzne dyski przenośne) oraz zdalne komputery, które mogą być objęte incydem
- Zebrać dane związane z ruchem sieciowym w określonym czasie. Sprawdzić stan aplikacji i systemów operacyjnych komputerów dotkniętych incydem.
- Zbadać pliki i aplikacje zaatakowanych serwerów.

2.2 Pozyskiwanie danych

Pozyskiwanie danych jest kolejnym etapem śledztwa. Należy przy tym pamiętać, że część danych jest bardzo wrażliwa i ulotna, dane te mogą być w łatwy sposób zniekształcone lub uszkodzone. Dlatego, powinniśmy upewnić się, że zostały one poprawnie zebrane i zabezpieczone.

2.2.1 Przygotowanie zestawu narzędzi do przeprowadzenia śledztwa

Do przeprowadzenia procesu zbierania danych, potrzebujemy zestawu narzędzi zarówno programowych (oprogramowanie) jak i sprzętowych (np. sprzętowy bloker). Taki zestaw może składać się z komputera przenośnego wraz z zainstalowanym oprogramowaniem. Musimy pamiętać również, o czystych nośnikach, takich jak płyty CD/DVD, wyczyszczone twarde dyski lub napędy z pamięcią typu flash. Coraz częściej zestaw narzędzi składa się z płyty boot'owalnej, na której znajduje się system operacyjny (dostępne są zarówno systemy oparte o Linux jak i Windows) wraz z niezbędnymi

narzędziami. Nie możemy zapomnieć o wszelkich kablach połączeniowych, takich, jak: kable sieciowe, zasilające, przejściówki do interfejsów IDE/SATA/SCSI oraz urządzenia umożliwiające wykonanie kopii danych w trybie tylko do odczytu ze źródłowego nośnika, tutaj możemy zastosować zarówno sprzętowe jak i programowe blokery.

2.2.2 Zbieranie danych

Zbieranie danych w postaci dowodów elektronicznych możemy przeprowadzić lokalnie, z fizycznym dostępem do badanego komputera lub poprzez sieć. Zdobywanie danych lokalnie posiada przewagę w postaci pełnej kontroli nad komputerem i zawartymi na tej maszynie danymi. Jednakże, sytuacja taka nie zawsze jest możliwa, szczególnie w przypadku zamkniętych serwerowni, pomieszczeń czy serwerów o wysokiej dostępności, takich, jak klastry z macierzami. Innym czynnikiem powodującym to, że badanie wykonywane jest zdalnie może być tajemnica śledztwa, charakter gromadzonych danych lub ramy czasowe prowadzonego badania.

Proces pozyskiwania danych powinien obejmować [MICROSOFT1]:

1. Utworzenie właściwej dokumentacji, która pozwoli ustalić autentyczność zebranych dowodów. Powinna ona zawierać takie informacje jak:
 - Kto wykonał daną czynność i dlaczego? Co przez to działanie próbowano osiągnąć, co spodziewano się wyjaśnić ?
 - Jak wykonywano daną czynność, jakich narzędzi użyto oraz według jakich procedur czy ustaleń działano ?
 - Kiedy dokładnie wykonano te czynności i co było wynikiem przeprowadzenia tych działań ?
2. Wybranie metody pozyskiwania danych. Przeważnie, jest to kombinacja zbierania danych online i offline. Zależy od tego, czy dane są ulotne czy nieulotne.
3. Ustalenie i opisanie potencjalnych źródeł danych, mogą to być:
 - Serwery. Pliki logów z urządzeń sieciowych wewnętrznej i zewnętrznej infrastruktury, takich jak zapory ogniowe, routery, serwery Proxy, systemy wykrywania włamań (IDS/IPS)
 - Komponenty sprzętowe takie jak karty sieciowe (posiadające adres fizyczny MAC) karty PC CARD lub USB, zewnętrzne porty, takie jak: FireWire, USB, lub PC Card.

- Urządzenia przechowujące dane, wewnętrzne i zewnętrzne (dyski twarde, taśmy, inne wymienne nośniki danych) jak również przenośne urządzeniach, takie jak: komórki, palmtopy, odtwarzacze MP3, pendrive'y czy aparaty fotograficzne.
4. Określenie kolejności, w jakiej będziemy gromadzić dane. Jest to szczególnie istotne, gdy musimy zbierać dane ulotne. Ustalenie metody zbierania danych z urządzeń magazynujących dane. Należy przy tym wziąć pod uwagę, że:
- Wyjęcie wewnętrznego urządzenia pamięciowego powinno być wykonane po odłączeniu komputera od źródła zasilania.
 - Wyjęcie dysku z podejrzanego komputera oznacza, że dane będą pozyskiwane we własnym systemie do zbierania danych. Nie zawsze jest to możliwe, gdyż dysk, może być częścią macierzy (np. RAID) lub innych urządzeń typu SAN, i wyjęcie dysku może wiązać się z całkowitą utratą danych.
 - Zaleca się utworzenie kopii bitowej dysku na naszym własnym nośniku, wykorzystując technikę kopii zapasowych, upewniając się, że dostęp do oryginalnych danych ustawiliśmy w trybie tylko do odczytu. Zaleca się wykonanie dokładnego opisu badanego urządzenia, załączając wszystkie informacje na temat konfiguracji (np. ustawienie zworek), rodzaju interfejsu, nazwy producenta, pojemności, typu i modelu urządzenia oraz jego numeru seryjnego.
5. Umożliwienie sprawdzenia poprawności zebranych danych. Można do tego wykorzystać sumy kontrolne (kryptograficzne funkcje skrótu) lub podpisy cyfrowe. Pozwalają nam one upewnić się, czy skopiowane dane są identyczne z oryginalnym nośnikiem.

2.2.3 Przechowywanie i magazynowanie zgromadzonych danych

Po zebraniu danych, które mogą stanowić dowód elektroniczny istotne jest zapewnienie im bezpiecznego miejsca do przechowywania. Można tutaj wykorzystać procedury archiwizacji danych istniejące w danej firmie.

Najlepsze praktyki podpowiadają nam następujące działania [MICROSOFT1]:

- Do składowania dowodów należy wykorzystywać pomieszczenia fizycznie chronione i zaplombowane.
- Należy zabezpieczyć wszelki dostęp do dowodów przed nieautoryzowanymi osobami zarówno fizycznie jak i poprzez sieć. Osoby mające dostęp do dowodów powinny być rejestrowane.

- Należy dodatkowo zabezpieczyć fizyczne nośniki poprzez umieszczenie ich w opakowaniach antystatycznych
- Zaleca się utworzenie, co najmniej dwóch kopii zebranych danych i przechowanie jednej z nich w bezpiecznej odległej lokalizacji
- Zaleca się zabezpieczenie dowodu zarówno fizycznie jak i cyfrowo (na przykład zabezpieczenie hasłem dostępu do nośników z kopią).
- Dla gromadzonych dowodów należy utworzyć dokument łańcucha zdarzeń. Powinien on zawierać listę nazwisk osób, które miały kontakt z dowodami, dokładną datę i godzinę pobrania dowodów do analizy i ich zwrotu.

2.3 Analiza danych

Mając zgromadzone dane można przystąpić do ich analizy. Metody używane do tego związane są z typem analizowanych danych.

2.3.1 Analiza danych sieciowych

W wielu przypadkach analizowanie danych sieciowych nie jest konieczne, ale zdarzają się przypadki, gdzie zbieranie takich danych jest bardzo istotne, np. gdy mamy do czynienia z serwerami świadczącymi usługi sieciowe. Jeśli taka analiza jest niezbędna, możemy posłużyć się następującymi procedurami [MICROSOFT1]:

1. Zbadanie logów usług sieciowych i zdarzeń skojarzonych z interesującymi nas usługami. Zazwyczaj ilości tych danych są bardzo duże, powinniśmy skupić się na konkretnych informacjach, takich jak nazwa użytkownika, data i czas oraz zasoby, do których dostał się intruz.
2. Zbadanie logów zapory ogniowej, serwerów proxy, systemu wykrywania włamań (IDS) oraz serwerów zdalnego dostępu. Wiele z tych logów zawiera informacje na temat połączeń przychodzących i wychodzących wraz z informacjami identyfikującymi dane działanie.
3. Dodatkowo można zbadać logi z monitorów sieciowych lub analizatora pakietów, jeśli takie dane są zbierane

2.3.2 Analiza danych znajdujących się na komputerze

Dane zawarte na komputerze lub serwerze zawierają informacje dotyczące systemu operacyjnego a także znajdujących się tam aplikacji. Procedury postępowania w tym wypadku [MICROSOFT1] powinny być wykonane w następującej kolejności:

1. W pierwszej kolejności musimy określić, czego poszukujemy, ponieważ możemy dysponować ogromną ilością danych, a tylko część z nich może być istotna w przypadku naszego incydentu.
2. Następnie należy zbadać dane systemu operacyjnego, włączając w to uruchomione aplikacje lub procesy. Powinniśmy zwrócić uwagę na programy, które zostały skonfigurowane do automatycznego uruchomienia podczas procesu uruchamiania komputera czy logowania się do systemu oraz przejrzeć opcje autostartu.
3. W kolejnym kroku należy przejrzeć uruchomione aplikacje i procesy wraz z ich zestawionymi połączeniami sieciowymi, poszukując procesów podejrzanych. Możemy tutaj posłużyć się narzędziami, które zostały opisane w rozdziale dotyczącym analizy danych ulotnych.

2.3.3 Analiza nośników danych

Nośniki danych, które zostały pozyskane podczas poprzedniej fazy zawierają wiele plików, naszym zadaniem jest analiza tych plików i wskazanie tych, które mogą być związane z naszym incydemtem. Musimy pamiętać, że to zadanie może okazać się zadaniem trudnym i zniechęcającym, szczególnie jeśli spojrzymy z perspektywy setek, czy tysięcy plików zawartych na dyskach twardych czy taśmach. Możemy tutaj posłużyć się najlepszymi praktykami [MICROSOFT1]:

1. Jeśli tylko jest to możliwe, powinniśmy pracować w trybie offline na kopii bitowej sporządzonej z oryginalnego dowodu.
2. Należy sprawdzić czy na dysku znajdują się zaszyfrowane dane, na przykład z użyciem EFS (*Encrypting File System*) w środowisku Windows⁹.
3. Pomocnym może być stworzenie diagramu struktury katalogów.
4. Interesują nas przede wszystkim pliki powiązane z incydemtem. W celu wyeliminowania tych, które nie uległy zmianie od momentu instalacji, można

⁹ Encrypting File System in Windows XP and Windows Server 2003 - <http://technet.microsoft.com/en-us/library/bb457065.aspx>

posłużyć się bazą NSRL (*National Software Reference Library*)¹⁰ zawierającą sumy kontrolne znanych plików systemowych i plików aplikacji. Pomocne mogą być również witryny informacyjne¹¹, na których znajdziemy informacje na temat znanych formatów plików, procesów, bibliotek dll i ich zastosowania wraz ze szczegółowym opisem.

5. Należy zbadać rejestr systemowy, zawierający konfigurację systemu Windows. To czego szukamy to procesy uruchamiane podczas startu systemu, zainstalowane aplikacje oraz informacje dotyczące nazwy użytkownika wykorzystanej do logowania się do domeny.
6. Kolejnym krokiem jest przeszukanie zawartości zebranych plików w poszukiwaniu plików powiązanych z naszą sprawą, uwzględniając tzw. alternatywne strumienie dane (ang. *Alternate Data Streams*¹²). Są to dodatkowe dane na partycjach NTFS umożliwiające stworzenie ukrytych plików pod innym plikiem czy folderem.
7. Po zidentyfikowaniu plików należy przeanalizować ich meta dane. Szczególną uwagę należy zwrócić na takie atrybuty plików, jak czasy utworzenia, ostatniego dostępu i ostatniego zapisu do pliku.
8. Kończącym krokiem jest przejrzanie zawartości wybranych plików za pomocą dostępnych przeglądarek plików, które pozwalają zapoznać się z zawartością pliku niezależnie od aplikacji, która była wykorzystana do jego utworzenia

2.4 Raport ze śledztwa

Jest to ostatni etap, będący podsumowaniem wykonanych prac. Składa się z dwóch kroków – uporządkowania pozyskanych informacji oraz sporządzenia raportu końcowego.

¹⁰ NSRL (National Software Reference Library) –<http://www.nsrll.nist.gov/> - witryna prowadzona przez amerykański Narodowy Instytut Standaryzacji i Technologii - NIST (National Institute of Standards and Technology) - bardzo duża bibliotek plików zawierająca metadane oraz dokładne informacje na temat plików spotkanych w systemach komputerowych. Witryna została stworzona po to aby wspomagać instytucje i prowadzone śledztwa

¹¹ Witryny pomocnicze – <http://www.filespecs.com>, <http://www.processlibrary.com/>, <http://www.wotsit.org/> oraz DLL help - <http://support.microsoft.com/dllhelp/Default.aspx> - baza danych zawiera informacje o plikach DLL dostarczanych z wybranymi produktami firmy Microsoft

¹² Alternatywne Strumienie Danych- dokładny opis wraz z przykładami zastosowania pokazał Harlan Carvey w pozycji [WFA]

2.4.1 Zgromadzenie i uporządkowanie pozyskanych informacji

Każda czynność wykonywana podczas komputerowego śledztwa musi być udokumentowana. Poniżej przedstawiono procedury, które pozwolą nam zebrać i uporządkować wymagane dokumenty w formie końcowego raportu [MICROSOFT1]:

1. Zebrać wszystkie dokumenty, notatki, zapiski czy uwagi sporządzone podczas fazy oszacowania, pozyskania i analizy danych. Określić te części dokumentacji, które mają znaczenie w dochodzeniu.
2. Wyszczególnić wszystkie fakty pomocne i istotne dla uzyskania wniosków, które zostaną uwzględnione w raporcie.
3. Utworzyć pełną listę dowodów, które będą przedstawione w raporcie.
4. Utworzyć spis wniosków, które mamy zamiar umieścić w raporcie.
5. Uporządkować i sklasyfikować informacje, które zostały zebrane i mogą być wykorzystane do poparcia wniosków. Same wnioski powinny być czytywiste i zwarte.

2.4.2 Utworzenie końcowego raportu

Bardzo istotne jest aby raport z przeprowadzonego dochodzenia był przejrzysty, zwarty, zrozumiały i skierowany do właściwej grupy odbiorców, którzy nie zawsze muszą mieć przygotowanie techniczne.

Raport powinien zawierać [MICROSOFT1]:

- **Cel raportu** – wyraźnie wskazany cel wykonania raportu, dla kogo został przygotowany, dlaczego został przygotowany.
- **Autor raportu** – wyszczególnienie autora i wszystkich osób biorących udział w dochodzeniu, podanie ich stanowisk oraz obowiązków przydzielonych podczas śledztwa.
- **Podsumowanie incydentu** – krótki opis incydentu wraz z wyjaśnieniem jego skutków. Streszczenie powinno być tak napisane, aby było zrozumiałe dla osób bez przygotowania technicznego.
- **Dowody** – przedstawienie opisu dowodów pozyskanych podczas śledztwa, każdy dowód powinien być opisany wraz z informacją jak został zdobyty i kto tę czynność wykonał.
- **Szczegółowe informacje** – przedstawienie szczegółowego opisu analizowanych dowodów wraz z dokładną informacją na temat analizy i metod zastosowanych

podczas tego procesu. Wyjaśnienie wyników ujawnionych podczas analizy, przedstawienie procedur, które poprzedzały cały proces dochodzenia oraz ujawnienie zastosowanych technik informatyki śledczej. Do opracowania należy dołączyć raporty z zastosowanych narzędzi oraz pliki logów potwierdzające słuszność naszych wniosków wraz z uzasadnieniem wniosków wyciągniętych na podstawie analizy. Każdy dokument dołączony do śledztwa powinien zawierać etykietę i musi być ponumerowany, co ułatwi poruszanie się po zgromadzonych materiałach.

- **Wnioski** – Jest to podsumowanie wyników śledztwa. Konkluzje powinny zawierać konkretne informacje przedstawione w postaci rezultatu dochodzenia. W celu poparcia każdego wniosku powinniśmy przytoczyć i wskazać dowód, ale bez zagłębiania się w szczegóły, tak jak to ma miejsce w sekcji „Szczegółowe informacje”. Do każdego wniosku powinniśmy dołączyć uzasadnienie, bazujące na zgromadzonych informacjach. Wnioski powinny być klarowne i jednoznaczne.
- **Dokumenty uzupełniające** – dołączenie dokumentów ogólnych i pośrednich odnoszących się do raportu, takich jak diagramy sieci, dokumenty opisujące przyjęte procedury lub opisujące standardy i technologie wykorzystane w dochodzeniu. Przewidywalnie raport będzie prezentowany różnym odbiorcom, warto rozważyć utworzenie i dołączenie słowniczka najtrudniejszych technicznych określeń użytych w raporcie, ma to szczególne znaczenie wtedy, kiedy raport będzie przedstawiany w sądzie.

3. ZBIERANIE DANYCH

Właściwe zebranie danych to podstawa poprawnie przeprowadzonego śledztwa. Im bardziej dokładne i pełne będą dane, tym lepsze i pełniejsze będą wnioski śledztwa. Podstawowa zasada, którą należy się kierować to zredukowanie do minimum ilości informacji, które mogą być nadpisane i utracone.

Zbierane dane można podzielić na ulotne i nieulotne. Dane ulotne (*ang. volatile data*) są to dane przechowywane w pamięci działającego systemu operacyjnego, i które mogą zostać utracone podczas zamknięcia systemu, odłączenia go od sieci bądź od zasilania. Dostęp do takich danych możemy mieć tylko jeden raz i od nas zależy, w jakim stopniu skorzystamy z tej możliwości. Dane nieulotne (*ang. non-volatile data lub persistent data*) – są to dane, które pozostają niezmiennie nawet wtedy, kiedy od systemu zostanie odcięte zasilanie lub zostanie on wyłączony, są to dane zapisane na stałe na dysku twardym lub innym nośniku informacji a także na płytach CD/DVD, dyskietkach oraz kluczach USB.

Ulotność danych powinna być uwzględniona podczas ich gromadzenia i wyznacza ona kolejność zbierania danych. Poniżej przedstawiono przykład¹³ kolejności uwzględniającej ulotność danych:

- Rejestry, pamięć podręczna (cache)
- Tablica routingu, arp cache, lista procesów, statystyki jądra, pamięć
- Tymczasowy system plików
- Dysk lub inny nośnik nieulotny
- Zdalne logi i dane monitoringu mogące być użyteczne podczas analizy systemu
- Konfiguracja fizyczna, topologia sieci
- Kopie zapasowe i archiwalne nośniki.

3.1 Przygotowanie do zbierania danych

Proces zbierania danych¹⁴ rozpoczynamy od przygotowania odpowiednich narzędzi w postaci zestawu do reagowania na incydenty (*ang. First Responder Toolkit*). Najczęściej

¹³ Kolejność taka zaproponowana została przez D.Brezinski & T.Killalea - w RFC3227

¹⁴ Opisany proces i sposób zbierania danych został zaproponowany przez autorów przewodnika [FRGCF]

jest to płyta CD/DVD lub dysk USB z zestawem programów i skryptów niezbędnych do analizy danych. Możemy skorzystać z już istniejącego zestawu, lub przygotować swój własny. Przykłady taki zestawów zostaną opisane i omówione w dalszej części pracy, jednak większość osób zajmujących się zawodowo informatyką śledczą posiada swój własny zestaw, który zawiera również narzędzia, których brakuje w gotowych zestawach.

Zakładając, że taki zestaw mamy już przygotowany, musimy przemyśleć i rozpocząć tworzenie dokładnej dokumentacji, która opisze każdy krok wykonany podczas analizy. Dokumentacja powinna zawierać przede wszystkim charakterystykę incydentu, czyli odpowiedzi na podstawowe pytania:

- Jak incydent został wykryty ?
- O której godzinie incydent miał miejsce ?
- Kto lub jaki czynnik pozwolił odkryć incydent ?
- Jaki sprzęt oraz jakie oprogramowanie znajduje się na podejrzanym komputerze ?
- Czy podejrzanym komputer jest kluczowy i krytyczny dla działania instytucji ?

Po scharakteryzowaniu incydentu powinniśmy zaplanować sposób prowadzenia zapisów z naszych działań (*ang. Forensic Collection Logbook*). Z uwagi na bardzo dużą ilość danych najwygodniej posługiwać się dokumentacją elektroniczną. Zanim rozpoczniemy działania musimy być w pełni świadomi, że jakiegokolwiek operacje wykonane na systemie plików analizowanego serwera, mogą zatrzeć i sfalszować dowody.

Pewne czynności muszą być jednak wykonane na badanym serwerze. Wtedy najbezpieczniejszym sposobem rozpoczęcia działań jest uruchomienie pliku zawierającego interpreter poleceń „cmd.exe” (właściwy dla danego badanego systemu) z płyty CD/DVD. Jeśli nie dysponujemy taką możliwością i uruchomimy wiersz linii poleceń z podejrzanego systemu, musimy zdawać sobie sprawę, że taki interpreter może być zmodyfikowany przez intruza lub wirus, a efekty działań mogą być inne niż się spodziewamy.

Wydawane polecenie związane jest z uzyskiwaniem danych o systemie. Są one zapisywane w logach. W celu składowania pliku z logami i plikami pomocniczymi najlepiej użyć wcześniej przygotowanego miejsca sieciowego na innym komputerze, w przypadku zaawansowanych działań możemy przygotować serwer specjalnie do tego

przystosowany (*ang. Forensic Server Project*¹⁵) lub w ostateczności możemy skierować wyniki naszych działań na dysk USB lub dyskiectę.

Jednym ze znanych sposobów na przekazywanie danych poprzez sieć jest użycie darmowego narzędzia **NETCAT**¹⁶ lub w przypadku konieczności szyfrowania transmisji **CRYPTCAT**¹⁷. Oba te narzędzia pozwalają na kopiowanie, wyświetlanie i łączenie kilku plików w jedną całość, wykorzystując do tego sieć opartą na TCP/IP.

Jeśli nie dysponujemy oprogramowaniem dedykowanym to możemy posłużyć się przekierowaniem „>” lub „>>”. Pierwsze z nich służy do stworzenia pliku lub jego nadpisania, drugie pozwala dopisać dane do już istniejącego pliku lub stworzyć nowy. Poniżej pokazano przykłady użycia przekierowania do zapisania listingu katalogu na innych maszynach lub nośnikach pamięci:

```
dir /ta > \\server\katalog\raport1.txt
```

lub

```
dir /ta >> h:\raport1.txt
```

gdzie h: to napęd USB lub zmapowany dysk sieciowy

Po wybraniu sposobu dokumentowania działań musimy zadbać o integralność i wiarygodność plików i dokumentów elektronicznych, stanowiących dowód pozyskanych informacji. Wiarygodność i integralność zapewniamy poprzez wyliczenie funkcji skrótu (*ang. hash*), wykorzystując jeden lub kilka dostępnych algorytmów, takich jak: MD5, SHA-1, SHA-256, Tiger czy Whirlpool. Do naszych celów wykorzystamy najpopularniejszy algorytm MD5¹⁸ lub SHA1¹⁹. W sieci możemy znaleźć wiele darmowych narzędzi tworzących skróty, takich jak **md5deep**²⁰ lub **FCIV**²¹. Przykład użycia konsolowej wersji **md5deep** przedstawiono poniżej. Program wykorzystano do utworzenia skrótu dla samego siebie:

```
C:\>md5deep.exe md5deep.exe  
7b17a3c9c31de090e59e275795b68df3 C:\md5deep.exe
```

¹⁵ Przykład takiego serwera napisanego w języku PERL zaproponował Harlan Carvey’a [WFIR]

¹⁶ NETCAT – uniwersalne narzędzie skanująco-monitorujące odpowiednik sieciowy unixowego polecenia cat - <http://www.vulnwatch.org/netcat/>

¹⁷ CRYPTCAT – rozszerzenie narzędzia NETCAT o możliwość szyfrowania przysyłanych danych - <http://farm9.org/Cryptcat/>

¹⁸ MD5 – Algorytm opisany w RFC 1321 przez R.Rivesta The MD5 Message-Digest Algorithm - <http://www.ietf.org/rfc/rfc1321.txt>

¹⁹ SHA1 – Algorytm opisany w RFC3174 przez D. Eastlake, P. Jones - US Secure Hash Algorithm 1 (SHA1) - <http://www.ietf.org/rfc/rfc3174.txt>

²⁰ Md5deep jest otwartym projektem prowadzonym przez Jesse Kornbluma - <http://md5deep.sourceforge.net/>

²¹ FCIV - File Checksum Integrity Verifier utility - <http://support.microsoft.com/kb/841290>

3.2 Dane ulotne

Dane ulotne mogą znajdować się w wielu miejscach, przede wszystkim w rejestrze systemowym, cache'u, pliku wymiany czy w pamięci RAM. Ta ostatnia zawiera uruchomione programy, procesy oraz usługi. Zawartość pamięci stale się zmienia i może zawierać bardzo dużo danych istotnych dla prowadzonego dochodzenia. Z uwagi na specyfikę i dynamikę danych zawartych w pamięci RAM zbieranie tych danych powinno odbywać się w czasie rzeczywistym na działającym systemie.

Innymi przykładami ulotnych danych są: historia wydanych poleceń, uruchomionych programów, czy otwartych dokumentów, lista zalogowanych użytkowników lokalnych i domenowych, lista otwartych plików, zawartość schowka.

Ilość danych ulotnych obecnych w danym momencie w systemie jest uzależniona w dużym stopniu od roli, jaką pełni dana maszyna. Jeśli jest to serwer usług, danych tych będzie więcej niż w przypadku zwykłej stacji roboczej. W tym wypadku do każdego serwera musimy podejść indywidualnie. Przykładami usług świadczonych przez serwery są: serwer plików, baz danych, poczty elektronicznej, usług WWW, ftp, VPN, zapory ogniowej (firewall), DNS, IDS, IPS oraz inne.

3.3 Proces zbierania danych ulotnych

Pozyskiwane dane ulotne możemy podzielić na dwa typy z uwagi na rodzaj danych:

- Zbiór informacji na temat bieżącej konfiguracji i bieżących stanów procesów i programów podejrzanego komputera;
- Zbiór informacji na temat stanu połączeń sieciowych.

Dane te zostaną przedstawione w kolejności ważności wraz z przykładowymi programami i poleceniami wspomagającymi ich pozyskanie i udokumentowanie.

3.3.1 Zbieranie informacji na temat bieżącej konfiguracji i stanów procesów

Bieżący czas i data – jest to najistotniejszy czynnik w prowadzonym badaniu; wszystkie czynności powinniśmy rozpocząć od sprawdzenia i zapisania dokładnego czasu, co do sekundy. W systemie dostępne są polecenia, które tej informacji dostarczają:

`time /t` (Windows²²) – wyświetla bieżący czas

`date /t` (Windows) - wyświetla bieżącą datę

lub po prostu

`time /t && date /t` – wyświetla obydwie informacje

`now` (Windows Server 2003 Resource Kit Tools²³) – wyświetla bieżącą datę i czas

Konfiguracja systemu, tzw. profil systemu – czyli wersja systemu, klucz, czas instalacji, startu, strefa czasowa, czas ciągłości działania (*ang. uptime*), katalog główny systemu Windows, wersja BIOS, ilość kart sieciowych i inne dane systemowe. Polecenia, które dostarczają tej informacji to:

`systeminfo` (Windows) – wbudowane polecenie wyświetlające informacje na temat konfiguracji systemu, numerów produktów, daty instalacji wraz z informacją na temat zainstalowanych poprawek.

`psinfo` (Sysinternals²⁴) – program zewnętrzny pokazujący czas działania systemu oraz listę zainstalowanych programów oraz poprawek. Program ten jest dość wszechstronny i pozwala również odpytywać system o zainstalowane programy lub wielkości twardego dysku.

`net statistics [workstation | server]` (Windows) – wbudowane polecenie systemowe do wyświetlania informacji na temat czasu działania systemu.

Bieżące procesy (ang. running processes) - sprawdzamy uruchomione procesy w celu zidentyfikowania podejrzanych procesów. Próbujemy również znaleźć procesy podszywające się pod procesy systemowe.

Harlan Carvey w swojej pracy [WFIR] rekomenduje zebranie i udokumentowanie następującego zestawu charakterystycznych cech każdego uruchomionego procesu:

²² (Windows) – oznacza polecenie wbudowane w system operacyjny Microsoft Windows

²³ Zestaw darmowych narzędzi Microsoft wspomagających pracę administratorów - <http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>

²⁴ Sysinternals – zestaw zaawansowanych narzędzi stworzonych przez Marka Russinovich'a i Bryce Cogswell'a, w chwili obecnej firmowanych przez firmę Microsoft <http://www.microsoft.com/technet/sysinternals/default.mspx>

- nazwa pliku wykonywalnego, którego obrazem jest uruchomiony proces
- folder, w którym znajduje się plik odpowiedzialny za uruchomienie procesu
- polecenie używane do uruchomienia danego procesu
- czas działania uruchomionego procesu
- kontekst, w jakim został dany proces uruchomiony
- lista modułów lub bibliotek dll, do których proces posiada dostęp
- ilość pamięci, jaką zajmuje dany proces.

Narzędzia pozwalające zdobyć te informacje przedstawiono poniżej:

netstat -ab (Windows) – wbudowane polecenie wyświetlające statystyki i bieżące połączenia protokołu TCP/IP, pozwala nam ustalić nazwy procesów używających portów protokołu TCP i UDP

listdlls (Sysinternals) – pozwala na wyświetlenie wszystkich plików DLL, które są obecnie załadowane wraz z numerem wersji oraz pełną ścieżką danej biblioteki

pslist (Sysinternals) – wyświetla informacje na temat procesów i wątków, między innymi informację jak długo dany proces jest uruchomiony

pulist (Windows 2000 Resource Kit²⁵) – program wyświetla listę procesów na zdalnym lub lokalnym komputerze

pmddump – (Ntsecurity.nu²⁶) - narzędzie to pozwala na dokonanie zrzutu pamięci zajmowanej przez wskazany proces, bez zatrzymywania tego procesu.

Pliki otwarte, startowe (autostart) oraz dane ze schowka - kiedy nasz system zostanie zainfekowany poprzez Trojana, rootkit'a lub inne oprogramowanie typu malware w systemie utworzone zostaną pliki umożliwiające autostart złośliwego oprogramowania po ponownym rozruchu systemu. Pliki te zostaną dodane do sekcji autostart lub rejestru. Żeby wychwycić taką sytuację musimy zebrać następujące dane:

- nazwy otwartych plików oraz ostatnio utworzonych dokumentów

²⁵ Windows 2000 Resource Kit - zestaw darmowych narzędzi Microsoft wspomagających pracę administratora, <http://www.microsoft.com/windows2000/techinfo/reskit/default.msp>

- znaczniki czasu (ang. *MAC Times*²⁷) towarzyszące krytycznym plikom i folderom.

Należy:

- Przejrzeć otwarte pliki w celu identyfikacji istotnych danych mogących mieć związek z naszym incydem
- Przeszukać krytyczne dane, takie jak hasła, obrazy oraz częściowe dokumenty zawarte w schowku
- Odszukać niecodzienne znaczniki czasowe w folderach systemowych oraz plikach startowych

Pomocne aplikacje i polecenia przedstawiono poniżej:

dir (Windows) – wbudowana komenda do wyświetlania listy plików

Przykład użycia:

```
dir c:\ /t: a /a /s /o:d,
```

gdzie opcje oznaczają:

/t: a – wyświetla pole znacznika czasu i używa tego pola do sortowania (dostępne znaczniki to: c – czas utworzenia, a – czas ostatniego uruchomienie lub otwarcia, w – czas ostatniego zapisu

/a - wyświetla wszystkie pliki wraz z plikami ukrytymi

/s - wyświetla wszystkie pliki w danym katalogu wraz ze wszystkim podkatalogami

/o:d – wyświetla pliki posortowane wg daty.

afind (Foundstone²⁸) – pozwala wyświetlić listę plików ostatnio uruchomionych bez ingerowania w znaczniki MAC, np. pliki uruchomione podczas dwóch ostatnich godzin

macmatch (Ntsecurity.nu) – narzędzie pozwalające na przeszukanie systemu plików biorąc pod uwagę datę ostatniego zapisu, dostępu lub utworzenia, bez modyfikacji tych znaczników.

²⁶ Ntsecurity.nu – witryna stworzona przez Arne Vidstrom zawierająca darmowe narzędzia systemowe

²⁷ MAC Times – jest częścią meta danych zawartych w systemie operacyjnym, do informacji tych zaliczamy „Modification” – określa kiedy dany plik został ostatnio zmodyfikowany, „Access” – pozwala nam sprawdzić, kiedy dany plik został uruchomiony lub otwarty do odczytu oraz „Creation” – czas utworzenia pliku w systemie

²⁸ Foundstone a division of McAfee - narzędzie to jest częścią „The Forensic Toolkit™ v.2.0”, dostępne na stronie <http://www.foundstone.com/us/resources-free-tools.asp>.

autorunsc (Sysinternals) – darmowe narzędzie, które pokazuje nam listę wszystkich plików startowych wraz z podziałem na sekcje startowe. Występuje w dwóch wersjach graficznej – **autoruns** oraz dostępnej z linii poleceń - **autorunsc**. Narzędzie to zdecydowanie przewyższa możliwości wbudowanego programu Windows **msconfig**. Program ten dostarcza nam obszerną informację na temat programów i samego procesu startu. Otrzymujemy pełną informację zawierającą sekcje: standardowe takie jak boot, logon, informacje znajdujące się w rejestrze oraz wiele innych np. rozszerzenie explorer, paski narzędziowe, usługi systemowe.

psfile oraz **handle** (Sysinternals) – oba te programy pozwalają wyświetlić otwarte pliki wraz z przypisanymi im uchwytami (*ang. file handle*).

pclip (Unxtools²⁹) – darmowy program pozwalający na zrzucenie zawartości schowka na ekran lub do pliku.

Użytkownicy zalogowani do systemu i aktualnie pracujący na serwerze – jeśli analizowaną maszyną jest serwer, wtedy kolejną czynnością jest sprawdzenie ilości aktualnie zalogowanych na nim użytkowników oraz określenie czasu pracy lokalnych i zdalnych użytkowników. Celem naszych poszukiwań będą:

- Ostatnio utworzone konta użytkowników
- Zwiększenie uprawnień już istniejącym użytkownikom
- Konta uprawnione do zdalnego dostępu ostatnio dodane lub modyfikowane
- Ilość użytkowników pracujących w czasie rzeczywistym i posiadających dostęp do systemu
- Czas pracy użytkowników z uwzględnieniem czasu zalogowania i wylogowania się z systemu, wraz z całkowitym czasem pracy na serwerze

Przydatne polecenia przedstawiono poniżej.

²⁹ Darmowe narzędzie zawarte w pakiecie unxutils – strona projektu <http://unxutils.sourceforge.net/>

net [users] (Windows) – wbudowane polecenie wyświetlające lokalnych i zdalnych użytkowników, komenda pozwala na dodawanie i modyfikowanie bazy użytkowników lokalnych

net [session] (Windows) – polecenie z tą opcją pozwala na uzyskanie informacji na temat połączeń użytkowników zdalnie podłączonych, wraz ze szczegółami połączenia takimi jak: adres IP, nazwa komputera, typ klienta oraz czas bezczynności.

netusers (SystemTools³⁰) – darmowe narzędzie, które pozwala na wyświetlenie aktualnie zalogowanych użytkowników lokalnych oraz pomaga nam wyświetlić informację na temat historycznych logowań użytkowników do danego komputera.

PsLoggedOn (Sysinternals) – darmowy program pokazujący zalogowanych użytkowników zarówno lokalnych jak i zdalnych

NTLast (Foundstone) – rozbudowane narzędzie do wyświetlania informacji na temat kont użytkowników oraz ich sposobu logowania się do systemu wraz z dokładnymi informacjami na temat udanych i nieudanych prób logowania. Program korzysta z logów systemowych.

DumpUsers (ntsecurity.nu) – program dość skomplikowany, ale pozwala nam na wyciągnięcie bazy użytkowników z komputera lub domeny, nawet wtedy kiedy opcje zabezpieczeń w rejestrze „RestrictAnonymous” są ustawione na ‘1’. Dla przypomnienia dodam, że RID³¹ konta administratora w systemach Windows wynosi ‘500’ i jest zawsze taki sam.

Biblioteki dynamiczne (DLL) i współdzielone – biblioteki DLL znajdują się w odrębnych plikach i zawierają skompilowane i połączone funkcje, które są wykorzystywane jednocześnie przez wiele procesów w tym samym czasie. System operacyjny mapuje daną bibliotekę DLL do zakresu adresów uruchomionego procesu

³⁰ Firma SystemTools Software Inc, udostępniła kilka darmowych narzędzi między innymi NetUsers <http://www.systemtools.com/free.htm>

podczas korzystania z tej biblioteki, co pozwala na wspólne wykorzystanie bibliotek przez wiele procesów lub programów. Narzędzie opisane poniżej pozwoli nam na identyfikację załadowanych do pamięci bibliotek oraz sprawdzenie czy dana biblioteka nie jest podstawioną biblioteką. Podczas poszukiwań zwracamy szczególną uwagę na:

- procesy, które używają uruchomionych bibliotek DLL
- nieznane biblioteki DLL
- porównanie listy bibliotek DLL załadowanych przez dany proces; sprawdzenia wymaga numer wersji biblioteki oraz data, która powinna być zgodna z datą instalacji systemu operacyjnego lub ostatnich poprawek

ListDLL (Sysinternals) – omawiane już wcześniej narzędzie wspomagające uzyskanie listy bibliotek DLL oraz porównania dwóch procesów i ich bibliotek DLL

3.3.2 Zbieranie informacji na temat stanu połączeń sieciowych

Otwarte porty i nawiązane połączenia sieciowe - diagnozę połączeń sieciowych należałoby rozpocząć od sprawdzenia wszystkich fizycznych kabli, kart sieciowych i towarzyszących im adresów IP. Nasze poszukiwania powinny obejmować:

- nieznane adresy IP i porty
- sprawdzenie prawdziwości połączeń i usług taki jak ssh, ftp, telnet, WWW
- wychwycenie połączeń typu tylna furka do systemu (*ang. backdoor*) na nieznanym portach
- sprawdzenie konfiguracji kart sieciowych.

W tym celu możemy się posłużyć następującymi narzędziami:

netstat -anb (Windows) – wbudowane narzędzie do wyświetlenia listy bieżących połączeń TCP/IP, dostarcza informacji o protokole, adresie IP, porcie oraz stanie połączenia, dodatkowo pokazuje identyfikator procesu PID po zastosowaniu parametru -o.

³¹ (RID) - identyfikator względny – (*ang. relative identifier*) – więcej informacji na temat identyfikatorów można znaleźć w dokumentacji do systemu Windows - http://www.microsoft.com/poland/windows2000/win2000serv/SYS_ROZ/roz12.msp

nbtstat (Windows) – wbudowane polecenie systemowe zbierające informacje na temat połączeń sieciowych wykorzystując protokół NBT (*NetBios over TCP/IP*), opcja -s pozwala nam wyświetlić tablicę sesji lokalnego systemu wraz ze zdalnymi adresami IP oraz zidentyfikować zmapowane połączenia dysków sieciowych.

NET share (Windows) – polecenie systemowe wyświetlające informacje na temat udziałów sieciowych zarówno udostępnionych na wybranym komputerze jak i aktywnych połączeń sieciowych do innych zasobów w sieci.

fport (Foundstone) – darmowe narzędzie listujące otwarte porty wraz z PID, nazwą procesu i ścieżką, z jakiej został uruchomiony dany proces.

PsService (Sysinternals) – darmowe narzędzie wspomagające zarządzanie usługami, program ten wyświetla status, konfigurację oraz zależności pomiędzy usługami, a także dodatkowo pozwala uruchomić, zatrzymać, wstrzymać, wznowić lub zrestartować usługi. Aplikacja pozwala nam pracować zarówno lokalnie jak i zdalnie. Dodatkowo narzędzie potrafi wyszukać w całej sieci specyficzne usługi takie jak DNS, DHCP oraz inne.

promisedetect (Ntsecurity.nu) – darmowa aplikacja, dzięki której możemy sprawdzić, czy karty sieciowe podejrzanego systemu pracują w trybie „promiscuous mode”. Tryb ten pozwala adapterom sieciowym na otrzymywanie i odczytywanie każdego pakietu przechodzącego przez ten adapter. Program ten jest bardzo pomocny w celu szybkiego sprawdzenia czy na danym systemie nie ma zainstalowanego analizatora pakietów (*ang. sniffer*), który działa właśnie w tym trybie.

ipconfig /All (Windows) – wbudowane polecenie do wyświetlenia bieżących szczegółowych informacji na temat adresów IP przypisanych do adapterów sieciowych, serwerów DNS, DHCP oraz adresów MAC.

Informacja na temat trasowania (*ang. routing*) – gromadząc dane o stanie połączeń sieciowych należy również przyjrzeć się bliżej bieżącej tablicy routingu, która może być zbudowana dynamicznie na podejrzanym komputerze, oraz tablicy pamięci podręcznej

ARP³², w której znajduje się informacja na temat ostatnich połączeń (odzworowań adresu IP na adres sprzętowy). Przydatne polecenia to:

netstat -r (Windows) – wskazywane już polecenie, które z opcją **-r** wyświetli aktualną tablicę routingu.

route print (Windows) – polecenie wyświetli nam bieżącą tablicę routingu, dodatkowo służy do zarządzania wpisami dokonywanymi w tablicy routingu.

arp -a (Windows) – wbudowane polecenie do zarządzania tablicą ARP, opcja **-a** wyświetla bieżące wpisy wskazując adresy IP, MAC oraz typ wpisu (dynamiczny lub statyczny).

3.4 Dane nieulotne

Dane nieulotne są to dane zapisane na stałe na dysku twardym lub innym nośniku informacji. Przykładem danych nieulotnych są pliki poczty elektronicznej, aktualne pliki i dokumenty użytkownika, ale również skasowane pliki. Dane tych ostatnich możemy znaleźć w obszarach tzw. „slack space”, plikach wymiany (*ang. swap*) oraz w nieprzydzielonych i nienadpisanych miejscach na dysku a także na wszelakich nośnikach z kopiami zapasowymi.

Gromadzenie danych nieulotnych oznacza poszukiwanie:

- plików i katalogów związanych z incydem (jawnych, ukrytych, zaszyfrowanych) oraz wszystkich informacji opisujących pliki, takich jak uprawnienia, data modyfikacji, etc.
- plików tymczasowych
- plików rejestru systemowego
- logów zdarzeń (*ang. events logs*)
- sektora bootowania (*ang. boot sector*)
- plików tymczasowych przeglądarek internetowych (*ang. cache*)
- plików ‘ciasteczek’ (*ang. cookies*) wysyłanych przez serwery www
- plików usuniętych, umieszczonych w „koszu na śmieci”

³² ARP (Address Resolution Protocol) – dokładny opis i specyfikację tego protokołu znajdziemy w RFC 826 - <http://www.ietf.org/rfc/rfc826.txt>

- plików zaplanowanych zadań
- plików kolejek wydruków
- plików podejrzanych o ukrywanie w nich informacji za pomocą technik steganografii.

3.5 Proces zbierania danych nieulotnych

Proces zbierania danych musi być dokumentowany. W dokumentacji powinniśmy umieścić wszelkie informacje na temat analizowanego komputera oraz bardzo szczegółowe informacje na temat nośnika, który będziemy analizować łącznie z opisem sposobu tworzenia kopii tego nośnika. Nośnikami danych mogą być:

- twarde dyski
- dyskietki, napędy ZIP, Jazz
- płyty CD/DVD
- pamięci FLASH (klucze USB, pendrive'y)
- karty pamięci (np. SD, MMC, MS, MS PRO, CF, MINI SD, XD, inne)
- dyski sieciowe
- taśmy
- palmtopy
- telefony komórkowe
- oraz inne.

Podstawową czynnością przed rozpoczęciem analizy jest wykonanie kopii w postaci obrazu dysku lub innego nośnika z danymi. Na potrzeby naszej analizy zajmiemy się dyskami twardymi. Tworzona kopia danych musi być wykonana ze szczególną starannością, bez dokonania żadnych zmian w oryginalnym nośniku. Jeśli dysk będzie stanowił dowód przestępstwa, to podłączając dysk w celu jego zbadania musimy zwrócić szczególną uwagę na to, aby dostęp do tego nośnika był tylko w trybie do czytania, jakkolwiek zapis danych na tym nośniku musi być zablokowany. Można w tym celu wykorzystać sprzętowe blokery (*ang. write blocking*). W chwili obecnej istnieje dużo

rozwiązań tego typu. Urządzenia takie są już dostępne w Polsce³³. W przypadku braku takiego urządzenia możemy skorzystać z komercyjnego oprogramowania lub musimy sami zadbać o to, aby w żaden sposób nie zmodyfikować danych zawartych na nośniku.

Proces klonowania dysków możemy wykonać na kilka sposobów:

- **Kopia dysk fizyczny --> dysk fizyczny** – metoda stosowana głównie do uruchomienia systemu z dysku
- **Dysk --> plik obrazu** – najbardziej popularny i najbardziej efektywny sposób przygotowania danych do dalszej analizy
- **Plik obrazu --> dysk fizyczny** – przywracanie z obrazu dysku fizycznego.

Przed rozpoczęciem wykonywania kopii musimy wybrać sposób fizycznego dostępu do dysku. Najlepszym sposobem jest fizyczne odłączenie dysku od komputera i podpięcie go pod sprzętowy bloker lub inny zaufany komputer. W przypadku braku takiej możliwości należy zadbać o bezpieczny sposób uruchomienia narzędzi do tworzenia obrazu dysku, np. wystartowanie komputera z bootowalnej płyty zawierającej system operacyjny DOS/Linux wraz z narzędziami do klonowania. Do wykonania duplikatu nośnika danych musimy podejść w szczególny sposób. W tym przypadku część popularnych programów do tworzenia obrazów może okazać się nie użyteczna, np. większość programów do obrazowania, wykonuje tylko obraz dysku lub partycji zawierający tylko aktualne pliki i wpisy w tablicy MFT (*ang. master file table*). Takie obrazy są zupełnie wystarczające do odtworzenia systemu z backupu, ale nie są wystarczające do analizy śledczej z uwagi na brak informacji o plikach skasowanych lub uszkodzonych.

Kopia nośnika powinna być wykonana bit po bicie (*ang. bit-for-bit*), uwzględniając całą strukturę logiczną oraz fizyczną dysku, mam tutaj na myśli kopie danych sektor po sektorze. Wykonany obraz do celów śledczych (*ang. forensic image*) powinien stanowić lustrzaną kopię nośnika źródłowego. Oprócz klastrów z danymi powinny zostać skopiowane pozostałe obszary takie jak, „resztki danych” (*ang. slack file*) oraz dane ukryte, częściowo usunięte, zaszyfrowane oraz obszary puste, jeszcze niezapisane danymi.

Proces duplikacji należy poprzedzić wykonaniem funkcji skrótu (*ang. hash*) na całym fizycznym dysku. Skrót ten posłuży do przyszłej weryfikacji czy dysponujemy

³³ Blokery sprzętowe firm: Intelligent Computer Solutions , Guidance Software , Tableau można znaleźć np. w sklepie internetowym <http://www.forensictools.pl/>

dokładną kopią oryginalnego dysku. Skróty te powinny być identyczne dla dysku źródłowego oraz jego kopii. Do wykonania funkcji skrótu najczęściej wykorzystuje się popularne algorytmy MD5 oraz SHA-1.

Najbardziej znane i dostępne narzędzia do duplikacji i wykonywania obrazów dysków pod przyszłą analizę przedstawiono poniżej:

dd (chrysocome.net³⁴) – darmowy i najbardziej popularny program do wykonywania obrazów dysków, znany głównie ze środowiska linuxowego, dostępny również w wersji konsolowej dla systemów Windows. Jedną z wersji możemy znaleźć w pakiecie UnxUtils³⁵ zaś rozbudowaną wersję znajdziemy w pakiecie FAU³⁶. W pakiecie tym dodatkowo otrzymujemy możliwość wykonania funkcji skrótu algorytmem MD5. Program „DD” pozwala nam na wykonanie kopii obrazu w formacie RAW, format ten jest obrazem nie zawierającym nagłówka oraz innych dodatkowych informacji.

Przykład użycia polecenia:

```
dd.exe if=\\.\PhysicalDrive0 of=d:\plik1.img
```

Opcja `if` określa dysk źródłowy, zaś opcja `of` plik z obrazem tego dysku.

FTK Imager (AccessData³⁷) – w pełni okienkowy program do tworzenia obrazów dysku. Program posiada wersję LITE, która w przeciwieństwie do wersji pełnej nie musi być instalowana na komputerze i może być uruchomiona z płyty CD lub dysku USB. Program ten jest wersją komercyjną, ale dopuszczalne jest również darmowe wykorzystanie w kilku przypadkach, szczegóły licencji dostępne są na stronie producenta. Program pozwala na wykonanie kopii:

- całego dysku fizycznego
- dysku logicznego (partycji)
- obrazu dysku (np. w celu konwersji formatów)
- zawartości pojedynczego folderu

³⁴ DD dla Windows dostępny na licencji GPL, na stronie projektu <http://www.chrysocome.net/dd>

³⁵ Zestaw narzędzi linuxowych dla systemu Windows, strona projektu <http://unxutils.sourceforge.net/>

³⁶ FAU – darmowy pakiet Forensic Acquisition Utilities stworzony przez George M. Garner Jr. w chwili pisania pracy dostępna była wersja RC3

³⁷ FTK Imager jest jednym z narzędzi firmy AccessData, z zestawu FTK (Forensic Toolkit) - <http://www.accessdata.com/common/pagedetail.aspx?PageCode=downloads>

Dodatkowo program ten pozwala na zapisanie i odczytanie obrazu w najbardziej popularnych formatach, szczegóły obsługiwanych formatów zostały umieszczone w tabeli 3.5.1.

Tabela 3.5.1 Obsługiwane formaty obrazów dysków w programie FTK Imager (źródło – dokumentacja do programu FTK Imager v.2.5.1)

Format pliku obrazu dysku	odczyt	zapis
dd RAW	■	■
EnCase E01	■	■
FTK Imager logical image	■	■
Ghost (tylko nieskompresowane obrazy dysku)	■	
ICS	■	
SafeBack (tylko do wersji 2.0)	■	
SMART (S01)	■	■

Dużo większe możliwości oferują komercyjne programy do wykonywania obrazów z nośników danych. Programy ten poza obsługą większej ilości formatów obrazu dysków, wspierają klonowanie dysków pracujących w macierzach sprzętowych oraz pozwalają na kopiowanie danych z taśm magnetycznych. Do tej grupy programów możemy zaliczyć:

EnCase Forensic (EnCase³⁸) – profesjonalny zestaw do analizy, zawierający narzędzie do tworzenia obrazu, oferujące zapis w wielu formatach. Narzędzie to pozwala również na podłączanie (ang. *mount*) utworzonych obrazów do systemu w celu dalszej analizy. Jedną z ciekawych opcji jest możliwość przekonwertowania obrazu do środowiska wirtualnej maszyny firmy VMware w celu uruchomienia systemu w środowisku wirtualnym z tak przygotowanego obrazu.

WinHex (x-ways.net³⁹) – prosty program będący edytorem dysków, wspomagający utworzenie obrazu zarówno z dysków twardych jak i bieżącej pamięci RAM. Jego zaleta jest niewielki rozmiar oraz szybkość.

SafeBack (NTI⁴⁰) – program do tworzenia lustrzanych kopii danych pomiędzy fizycznymi dyskami lub obrazów do dalszej analizy. Program w wersji konsolowej.

³⁸ Produkt firmy Guidance Software, Inc. - http://www.encase.com/products/ef_index.aspx

³⁹ Produkt firmy X-Ways Software Technology AG - <http://www.x-ways.net/winhex/index-m.html>

Ilook Investigator (Ilook⁴¹) – a właściwie to jego część dotycząca duplikowania danych - IXimager - Ilook External Imager. Program o dużych możliwościach, używany głównie przez instytucje rządowe i znany w środowisku prawniczym i sądowym w USA.

ByteBack (toolsthatwork.com⁴²) - aplikacja dostępna w postaci obrazu płyty bootowalnej lub dyskietki, pozwala na zastosowanie funkcji chroniącej przed zapisem (ang. *write block*) podczas tworzenia kopii obrazu dysku

⁴⁰ Produkt firmy New Technologies, Inc () - <http://www.forensics-intl.com/safeback.html>

⁴¹ Produkt firmy IRS Criminal Investigation Electronic Crimes Program and Elliot Spencer - <http://www.ilook-forensics.org/>

⁴² Narzędzie firmy Tech Assist, Inc) - <http://www.toolsthatwork.com/byteback.htm>

4. ANALIZA ZGROMADZONYCH DANYCH

Analiza zgromadzonych danych jest procesem dość skomplikowanym i czasochłonnym, ponieważ nie można przewidzieć i poukładać sobie planu działania. Bardzo często rozpoczęcie poszukiwań rozpoczyna się od drobnych wskazówek lub sugestii osoby zlecającej taką analizę. Prace związane z przygotowaniem i zabezpieczeniem plików i obrazów dysków miały na celu przygotowanie danych do dalszej obróbki. Proces analizy przypomina pracę detektywa, który rozpoczyna pracę od rozpoznania sprawy i poprzez kolejne drobne kroki, stara się dojść do sedna sprawy i rozwikłać zagadkę.

4.1 Typy i rodzaje szukanych danych

Analizę zazwyczaj rozpoczyna się od podstawowych plików reprezentujących znane i podstawowe dokumenty elektroniczne, takie jak:

- pliki dokumentów biurowych
- pliki zawierające pocztę elektroniczną
- pliki graficzne
- pliki skompresowane (archiwa)
- pliki baz danych
- pliki muzyczne
- pliki filmów i animacji
- pliki skryptów
- pliki aplikacji i programów
- pliki projektów, schematów
- pliki komunikatorów internetowych
- pliki tymczasowe
- pliki stron internetowych
- pliki kolejkowania wydruku
- pliki ukryte w plikach graficznych (steganografia)
- pliki zaszyfrowane
- pliki typu ciasteczka (ang. *cookies*)
- partycje/ pliki wymiany

- logi i rejestry
- dane przeglądarki
- dane skasowane
- dane i pliki z backupu
- oraz wiele innych.

4.2 Charakterystyczne miejsca do poszukiwania danych

Podstawowe zmienne systemowe

Dane opisujące charakterystyczne miejsca systemu plików zawarte są w zmiennych środowiskowych. Wartości te dla danego systemu możemy wyświetlić w poprzez wywołanie komendy „SET” z linii poleceń. Najważniejszymi zmiennymi przydatnymi w omawianej analizie są:

```
ALLUSERSPROFILE=C:\Documents and Settings\All Users
ComSpec=C:\WINDOWS\system32\cmd.exe
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\Administrator
SystemDrive=C:
SystemRoot=C:\WINDOWS
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS
```

Zmienne środowiskowe to ciągi znaków zawierające informacje o środowisku systemu Windows oraz o aktualnie zalogowanym użytkowniku. Niektóre procesy i programy korzystają z tych parametrów w celu zlokalizowania, gdzie mają umieszczać pliki lub przeszukiwać określone miejsca (np. pliki tymczasowe). Domyślny instalator systemu Windows konfiguruje zmienne systemowe, np. domyślną lokalizację systemu Windows.

Domyślny folder systemowy (ang. *System Folder*) – jest to miejsce, w którym znajdziemy zainstalowany system Windows wraz z plikami konfiguracyjnymi. Nazwy folderów przybierały różne nazwy w zależności od wersji systemu, pełne zestawienie domyślnych folderów znajdziemy w tabeli poniżej.

Tabela 4.2.1 Domyślne nazwy folderów tworzone podczas instalacji systemów Windows (źródło – [EnCase])

System Operacyjny (Operating System)	Folder zawierający Profil Użytkownika (User Profile Folders) <u>Zmienna systemowa: USERPROFILE</u>	Domyślny folder systemowy (Default System Folder) <u>Zmienne systemowe: SystemDrive, SystemRoot, windir</u>
Windows 9x/Me	Nie występował Documents and Settings	C:\Windows
Windows NT	Nie występował. Documents and Settings / C:\WINNT\Profiles	C:\WINNT
Windows 2000	C:\Documents and Settings	C:\WINNT
Windows XP/2003	C:\Documents and Settings	C:\Windows
Windows Vista/2008	C:\Users	C:\Windows

Profil użytkownika (ang. User Profile Folder) – jest to folder, w którym w systemach Windows przechowywana jest informacja na temat użytkownika, jego ustawień, dokumentów, pulpitu oraz plików tymczasowych, zarówno dotyczących tworzonych dokumentów jak i ściąganych plików internetowych. W profilu przechowywane są również pliki poczty elektronicznej, oraz inne charakterystyczne ustawienia dla programów spersonalizowane dla konkretnego użytkownika. Z punktu widzenia analizy jest to podstawowe miejsce, do którego należy zajrzeć w celu zbadania poczynań użytkownika.

Profil każdego użytkownika kryje w sobie kilka charakterystycznych miejsc, do których warto zajrzeć i przyjrzeć się bliżej zawartym tam plikom.

Pulpit (ang. Desktop) – jest to folder, znajdujący się w głównym katalogu profilu, i jest tworzony podczas procesu tworzenia profilu użytkownika. W początkowej fazie folder ten jest mały i zawiera tylko skróty do innych dokumentów i aplikacji. Jednakże użytkownicy systemów Windows upodobali sobie ten folder do umieszczania w nim również plików, bo przede wszystkim pulpit jest w zasięgu ich wzroku i „pod ręką”, o ile Administrator nie zabronił zapisu w tym folderze nadając stosowne uprawnienia.

Moje Dokumenty / Dokumenty (ang. My Documents/Documents) – katalog umieszczony w głównym katalogu profilu użytkownika, przeznaczony na pliki tworzone przez użytkownika. Folder ten zawiera podkatalogi: moja muzyka, moja obrazy oraz wiele

innych, które uzależnione są od zainstalowanej wersji systemu oraz wersji aktualizacji zbiorczej (ang. *service pack*). Większość aplikacji próbuje domyślnie zapisywać w nim pliki stworzone przez użytkownika. Folder ten może być przekierowany do innego folderu na tym samym dysku bądź do innej lokalizacji sieciowej.

Temp – folder plików tymczasowych, zlokalizowany jako podkatalog folderu USTAWIENIA LOKALNE (ang. *LOCAL SETTINGS*), w systemach Vista folder ten znajduje się w lokalizacji “Users\%UserName%\AppData\Local\Temp”. Katalog ten przeznaczony jest na pliki tymczasowe. W miejscu tym znajdziemy na przykład tymczasowe kopie otwartych dokumentów. Niektóre programy zmieniają rozszerzenia plików tymczasowych i wykasowują je po skończonych operacjach, jednak część programów po prostu postawia je w tym miejscu. Folder ten bardzo często wykorzystywany jest przez programy instalacyjne do tymczasowego rozpakowania plików instalacyjnych. Zatem w tym miejscu możemy znaleźć pliki będące śladami po zainstalowanych aplikacjach, pomimo odinstalowania programu.

Ulubione (ang. *Favorites Folder*) – w folderze tym znajdziemy łącza do stron internetowych, które zostały zapisane przez użytkownika do listy ulubionych w przeglądarce.

Ciasteczka (ang. *Cookies Folder*) – folder zawiera małe pliki tekstowe zapisywane przez serwery WWW, w celu identyfikacji użytkownika i zapisywania informacji związanych z danym użytkownikiem. Pliki te pozwalają na kontrolę i monitorowanie użytkowników, pozwalają zapamiętać login użytkownika i ogólnie ułatwiają proces ponownego zalogowania się na stronach WWW. W systemach Windows XP katalog ciasteczek znajduje się w głównym katalogu profilu, a w systemach Vista – w katalogu „Users\%UserName%\AppData\Roaming\Microsoft\Windows\Cookies” oraz wewnątrz podkatalogu „Low” zawartego w katalogu (..\cookies\). Pliki te zawierają datę ich modyfikacji przez serwery WWW oraz datę wygaśnięcia.

Przykładem pomocnego programu do analizy plików ciasteczek jest darmowa aplikacja **CookieView - Cookie Decoder**⁴³ oraz **IECookiesView**⁴⁴

⁴³ Program firmy Digital Detective <http://www.digital-detective.co.uk/freetools/cookieview.asp>

⁴⁴ Darmowy program firmy NIRSOFT - <http://www.nirsoft.net/utills/iecookies.html>

Katalog History – w systemie Windows XP folder ten zlokalizowany był w profilu użytkownika w podkatalogu \Ustawienia lokalne (ang. *Local Settings*), w systemie Windows Vista, ten podkatalog to:

c:\Users\%User name%\AppData\Local\Microsoft\Windows\History.

Folder ten zawiera historię przeglądanych witryn. Charakterystycznym plikiem jest **index.dat**, który jest bazą danych przeglądanych stron oraz źródłem cennych informacji na temat odwiedzanych witryn. Plik ten w zależności do wersji Windows występuje w kilku miejscach i obejmuje różny zakres przeglądanych stron. Pomocnym przy analizie tego pliku mogą okazać się programy: **IEHistoryView**⁴⁵ oraz **Index.dat Analyzer 2.5**⁴⁶, a także starsze programy Pasco czy Galleta.

Tymczasowe pliki internetowe (ang. *Temporary Internet Files*) – w folderze tym przetrzymywane są kopie plików powiązane z odwiedzonymi stronami. Są to między innymi pliki o rozszerzeniach: jpg, png, gif, htm, html, css, js, xml oraz wiele innych. Pliki te pozwalają przybliżyć, jakie strony i z jakimi treściami były odwiedzane przez danego użytkownika. W dużym stopniu są to pliki graficzne, po przejrzaniu, których można szybko wyciągnąć wnioski co do oglądanych witryn. Pomocnym programem może okazać się program **IECacheView**⁴⁷

Swap File – systemy Windows używają tego pliku w przypadku wykorzystania całej pamięci RAM. Pamięć wykorzystywana przez system jest zrzucana do pliku „pagefile.sys” - bardziej formalna nazwa dla tego typu plików. Plik ten przeważnie znajduje się w katalogu głównym dysku systemowego, ale może być skonfigurowany i przeniesiony w inne miejsce. W systemach Windows możemy spotkać się z sytuacją, kiedy po zamknięciu plik ten będzie czyszczony (klucz rejestru **HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management** będzie miał ustawioną wartość **ClearPageFileAtShutdown** na 1). W pliku tym możemy znaleźć informacje, które były zapisane w pamięci RAM ale mogły nigdy nie trafić na dysk twardy. Również w tym pliku

⁴⁵ IEHisotryView - http://www.nirsoft.net/web_browser_tools.html

⁴⁶ Index.dat Analyzer 2.5 - <http://www.systemance.com/indexdat.php>

⁴⁷ IECacheView - http://www.nirsoft.net/web_browser_tools.html

możemy znaleźć częściowo odszyfrowane informacje, które na dysku są przechowywane w postaci zaszyfrowanej.

Hibernation File – plik hibernacji „hiberfil.sys” wykorzystywany do usypiania komputera bez systemowego zamknięcia. Podczas tej operacji pamięć RAM zostaje zrzucona do pliku, tak aby po ponownym wybudzeniu komputera, przywrócić komputer do pracy w stanie w jakim został on uśpiony. Cała pamięć RAM zostaje przywrócona z pliku. Z perspektywy analizy możemy tam znaleźć wiele cennych informacji.

4.3 Pliki skompresowane ZIP,RAR,CAB, etc.

Coraz częściej na dyskach można znaleźć pliki spakowane w różnych formatach, warto takie pliki rozpakować i przyjrzeć im się dokładniej. Pliki zawarte w archiwum to nie tylko wersje instalacyjne programów, ale również pliki, które są poddawane kompresji przed wysłaniem ich przez Internet np. pocztą elektroniczną lub klientem FTP. Pliki te mogą być kopią istotnych danych. Z uwagi na różnorodność formatów, należy przyjrzeć się dokładniej ich rozszerzeniom i wielkościom, bardzo często są to duże archiwa, które po rozpakowaniu mogą zająć od 2 do 10 razy więcej miejsca niż wielkość spakowanego archiwum.

4.4 Poczta elektroniczna pliki charakterystyczne

W obecnych czasach poczta elektroniczna stanowi podstawowe medium przekazów elektronicznych, za pomocą poczty dziś przekazywane jest wszystko, od śmiesznych filmów, poprzez bardzo ważne kontrakty, czy oferty handlowe. Najbardziej popularnymi programami do odbioru poczty elektronicznej w systemach Windows są: Outlook Express (Windows Mail zawarty w Microsoft Vista) oraz Microsoft Outlook, który najczęściej wykorzystywany jest wraz z pakietem Microsoft Office. Charakterystyczne pliki dla poczty Outlook Express to pliki o rozszerzeniu .dbx, istnieje wiele programów, które pomogą nam przejrzeć pocztę zawartą w tych plikach. Musimy pamiętać, iż w systemie Vista i produkcie Windows Mail, rozszerzenie to już nosi nazwę .eml (skrót od email) i domyślnie pliki znajdują się w profilu użytkownika a dokładniej:

- Outlook Express – C:\Documents and Settings\%Username%\Application Data\Identities

- Windows Mail – c:\Users\%username%\AppData\Local\Microsoft\Windows Mail\Local Folders\

Program Microsoft Outlook – w zależności od konfiguracji aplikacji może tworzyć pliki o rozszerzeniu **.pst** (ang. *Outlook Personal Folder File*) lub **.ost** (ang. *Exchange Offiline Cache*). W drugim przypadku korzystamy z poczty opartej o produkt Microsoft Exchange. Pliki .pst są dość popularnym formatem i często możemy spotkać je na komputerach firmowych ale także na komputerach domowych. Pliki .pst mogą być plikami zabezpieczonymi hasłem, ale usunięcie tego hasła dziś nie stanowi większego problemu, można wykorzystać do tego chociażby darmowy program **PstPassword**⁴⁸. Plik .pst jest plikiem bazy danych, w którym usunięcie emaili nie usuwa ich trwale z pliku, a tylko oznacza jako usunięte. W przypadku, kiedy użytkownik nie skorzysta z funkcji kompaktowania pliku pst, można spróbować odzyskać skasowane pliki, np. za pomocą komercyjnej aplikacji **RecoverMyEmail**⁴⁹.

Musimy pamiętać o innych produktach do obsługi poczty elektronicznej takich jak: GroupWise, Eudora, The Bat, Mozilla Thunderbird, Pegasus Mail, Incredimail czy wiele innych, które również mają swoje pliki.

Dość trudnym do wykrycia i analizy jest konto pocztowe, wykorzystywane poprzez witrynę WWW, w takim przypadku pozostaje nam dość szczegółowa analiza odwiedzanych stron oraz analiza plików tymczasowych, w których możemy znaleźć pliki pobrane i otworzone na lokalnym komputerze.

4.5 Alternatywne strumienie danych

Alternatywne strumienie danych (ang. *Alternate Data Stream*) jest to własność systemu plików NTFS (używana już od Windows NT 3.1), nie zawsze znana Administratorom i użytkownikom. Funkcjonalność ta została stworzona w celu kompatybilności z systemem plików HFS Macintosh. W systemie tym każdy plik mógł posiadać stowarzyszony z nim drugi plik (nazywany rozwidleniem, ang. *fork*), w którym przechowywane były tzw. dane zasobów, pomocnicze w stosunku do danych przechowywanych w pliku. Mogły to być na przykład czcionki czy elementy graficzne. W systemie NTFS takich stowarzyszonych ze sobą plików może być wiele. Noszą one nazwę strumieni. Każdy plik w systemie NTFS

⁴⁸ PstPassword - http://www.nirsoft.net/utills/pst_password.html

⁴⁹ Recover My Email - <http://www.recover-my-email.com/> - wersja trial

posiada przynajmniej jeden strumień :\$DATA. Alternatywny strumień to po prostu inny plik podpięty do istniejącego pliku lub katalogu. Technikę tę można wykorzystać do ukrywania programów i danych.

Tworzenie plików ukrytych techniką ADS, to dodanie nowego pliku do istniejącego pliku jako inny strumień. Strumienie oddzielane są znakiem dwukropka „ : ”. Aby utworzyć ukryty plik tekstowy przypisany do już istniejącego pliku plik.txt za pomocą notatnika, wystarczy użyć polecenia:

```
C:\Windows\system32\notepad.exe c:\plik.txt:plik_ukryty.txt
```

Program **notepad** zapyta nas czy ma utworzyć nowy plik i jeśli potwierdzimy, taki plik zostanie utworzony. W systemie pozornie nic się nie zmieni, ukryty plik nie będzie wykazany w listingu katalogu, rozmiar pliku pierwotnego nie ulegnie zmianie. Ponowne wydanie polecenia w postaci podanej powyżej otworzy ukryty plik.

Do kopiowania zawartości plików nie tylko tekstowych ale również binarnych, możemy posłużyć się poleceniem **type**, np.

```
type C:\WINDOWS\system32\calc.exe > plik.txt:plik_ukryty.exe
```

Tak przygotowany i ukryty plik, możemy uruchomić w systemie Windows XP, za pomocą komendy:

```
start .\plik.txt:plik_ukryty.exe.
```

W systemie Windows Vista, taki sposób już nie zadziała z uwagi na wprowadzone zabezpieczenia ale zamiast plików wykonywalnych możemy nadal uruchomić skrypt VBS (ang. *visual basic script*) za pomocą komendy:

```
wscript .\plik.txt:skrypt.vbs.
```

Przedstawioną funkcjonalność upodobało sobie wiele programów takich jak wirusy, programy złośliwe, spyware czy programy do wysyłania spamu, dlatego też warto za każdym razem sprawdzić badany komputer czy nie zawiera ukrytych plików bądź aplikacji w ADS.

Wykrywanie ukrytych plików w starszych systemach Windows (Windows XP, Windows 2003 i starsze), jest trudne i niemożliwe bez zewnętrznych narzędzi. Jeśli przyjrzymy się ukrytemu plikowi, to znanymi narzędziami w systemie Windows nie jesteśmy w stanie podejrzeć alternatywnego strumienia, a co za tym idzie ukrytych danych. Kliknięcie na pliku i wybranie opcji „Właściwości” zawsze pokaże nam tylko właściwości głównego pliku. Dodatkowo musimy pamiętać, że ADS może zostać również przypisany do katalogu.

Narzędzi do wykrywania plików ADS istnieje wiele, najbardziej popularne i darmowe to: **STREAMS**⁵⁰ oraz **LADS**⁵¹. W systemach Windows Vista i Windows 2008 Server możemy skorzystać z wbudowanego polecenia **DIR /R**, które wyświetli informacje o dodatkowych strumieniach.

4.6 Pliki graficzne i steganografia

Pliki graficzne od zawsze kryły w sobie wiele tajemnic i były źródłem ukrywania informacji. Techniki ukrywania informacji znane są od bardzo dawna, chociażby technika nakłuwania liter w dostarczonej stronie tekstu, po odczytaniu w odpowiedniej kolejności nakłutych liter, otrzymywaliśmy klucz, który mógł posłużyć do deszyfrowania danych. Innym przykładem, w bliższych nam czasach, jest długopis, który posiada tusz niewidzialny dla ludzkiego oka, a więc nie zostawiający śladów po napisaniu, ale jeśli tak napisany tekst obejrzymy w świetle ultrafioletowym, to nagle na kartce ukazuje się czytelny tekst, niewidoczny w normalnym świetle.

Steganografia – jest to technika ukrywania informacji w istniejących plikach, np. graficznych, w sposób nie pogarszający obrazu widzianego przez ludzkie oko. Wykorzystywana jest tutaj kompresja obrazu pogarszająca jego jakość, tak aby na pierwszy rzut oka nie można było odróżnić obrazów przy porównaniu z oryginałem. Innym spotykanym rodzajem plików, w których ukrywa się dane są pliki dźwiękowe. Mogą to być również pliki tekstowe.

Najczęściej stosowanym i dobrze nadającym się do ukrywania danych formatem plików graficznych jest mapa bitowa (ang. *bitmap*) reprezentująca rastrowy sposób prezentacji grafiki, GIF (ang. *Graphics Interchange Format*) czy nowszy format PNG (ang. *Portable Network Graphics*), w którym można stosować bezstratne algorytmy kompresji danych. Pliki skompresowane przy pomocy algorytmów JPEG, nie nadają się do tego typu działań, ponieważ już są dość dobrze skompresowane i nie uda się ukryć w nich danych bez widocznego pogorszenia jakości obrazu.

Główną zaletą tej techniki jest umożliwienie przesyłania ukrytych informacji publicznymi kanałami przekazywania danych, takimi jak darmowe skrzynki email, czy witryny WWW. Pozornie wyglądające na pierwszy rzut oka zdjęcie przedstawiające

⁵⁰ STREAMS - <http://technet.microsoft.com/en-us/sysinternals/bb897440.aspx>

⁵¹ LADS - *List Alternate Data Streams* - <http://www.heysoft.de/nt/ep-lads.htm>

krajobraz wakacyjny czy fotografię osoby, może skrywać zaszyfrowany plik lub wiadomość. W przeprowadzonym badaniu zostanie pokazana ta technika w praktyce.

Na temat steganografii można napisać kolejną pracę lub dość obszerną książkę opisującą możliwości i techniki ukrywania informacji, korzystające z najnowszych i trudnych do złamania algorytmów stosowanych do szyfrowania informacji, takich jak: IDEA, 3DES czy AES. Korzystając z wyszukiwarki Google.com, znajdziemy bardzo dużo programów, które pozwalają na stosowanie tej techniki od najprostszych, które umożliwiają tylko umieszczenie jednego pliku w innym, po skomplikowane i komercyjne aplikacje, które mogą również odkrywać ukryte informacje przy pomocy technik typu „brute force”.

W przypadku Informatyki śledczej istotne jest ustalenie w pierwszej kolejności, czy w podejrzanym pliku znajduje się ukryta informacja lub plik binarny a następnie czy można ją odkodować. Przykładami aplikacji, które potrafią umieścić i ukryć informacje w pliku graficznym są programy: **S-TOOLS**⁵², **TROJAN IMAGE SECURITY**⁵³, **STEGDETECT**⁵⁴, **NCrypt TX 2.2**⁵⁵. Do automatycznego wyszukiwania i odszyfrowania musimy użyć zaawansowanych komercyjnych pakietów, takich jak np. ENCASE.

4.7 Rootkity

Rootkity (ang. *rootkits*) – jest to dość groźne i trudne do wykrycia oprogramowanie, które próbuje ukryć swoją obecność w systemie, bardzo często zastępując oryginalne programy, biblioteki czy wpisy w rejestrze. Oprogramowanie to jest swego rodzaju nową generacją programów złośliwych, które są niewykrywalna przez większość programów antywirusowych i są bardzo trudne do usunięcia.

Rootkity mogą działać w trybie użytkownika (ang. *user-mode*), naśladując i pełniąc rolę programu typu trojan, który przejmuje aplikację lub proces systemowy i wykonuje zadania przejętego programu, poprzedzając go swoimi działaniami lub w dużym stopniu zniekształcając te działania. Jako przykład możemy przywołać zainfekowany program **NETSTAT**, który oryginalnie wyświetla listę aplikacji i otwartych portów, natomiast zainfekowany program, może wyświetlać wszystkie połączenia oprócz tych, które sam nawiązał do innym systemów.

⁵² S-TOOLS - <http://www.spychecker.com/program/stools.html>

⁵³ TROJAN IMAGE SECURITY - <http://www.brothersoft.com/trojan-image-security-50247.html>

⁵⁴ STEGDETECT - <http://www.outguess.org/download.php>

⁵⁵ NCrypt TX - <http://www.littlelite.net/ncrypt/mainframe.html>

Dużo groźniejszym typem rootkitów są programy działające w trybie jądra systemowego (ang. *kernel-mode*). Ingerują one głęboko w system, łącznie z przetwarzaniem i zniekształcaniem danych wejściowych dostarczanych w strukturach danych, przez co stają się bardzo trudne do wykrycia i usunięcia. Bardzo często część tego typu programów jest napisana niewłaściwie i powodują częste BSoD (ang. *Blue Screen of Death*), potocznie nazywane „blue screenami” (nazwa pochodzi od niebieskiego koloru ekranu, na którym jądro systemu zwróciło błąd systemowy) i komputer przeważnie restartuje system, jeśli obsługa BSoD, nie jest ustawiona w inny sposób.

Do tego typu oprogramowania dołączył również kolejny typ rootkitów – komercyjny. W 2005 roku Mark Russinovich⁵⁶, wykrył i podał do publicznej wiadomości stosowanie i wykorzystywanie przez firmę SONY Corporation rootkity, które kontrolowały i zabezpieczały wydawane przez nich utwory muzyczne, chroniąc w ten sposób prawa intelektualne do utworów cyfrowych w technologii DRM (ang. *Digital Rights Management*). Najważniejszą kwestią był fakt, że użytkownik nie został powiadomiony przez wspomnianą firmę o stosowaniu oprogramowania, które bez zgody i wiedzy właściciela systemu instalowało się na jego komputerze i śledziło poczynania z chronionymi utworami. Firma Sony została ostro skrytykowana za takie praktyki i doszło do wielu procesów zakończonych dotkliwymi karami finansowymi dla firmy SONY⁵⁷. Tak, jak pokazał przykład firmy SONY, oprogramowanie to jest bardzo trudne do wykrycia i stanowi pole do działania dla hakerów, intruzów czy użytkowników pragnących ukryć swoje działania.

Na rynku powstało wiele programów zarówno komercyjnych jak i darmowych do wykrywania rootkitów. Należą do nich: **ROOTKIT REVEALER**⁵⁸, **SOPHOS ANTI-ROOTKIT**⁵⁹ czy **GMER**⁶⁰. W celu głębszej analizy tematyki rootkitów i zapoznania się z przykładowymi rootkitami, zachęcam do zapoznania się z witryną <http://rootkit.com/>, gdzie znajdziemy bardzo dużo informacji dotyczącej tej tematyki oraz sposobów wykrywania ich w systemach Windows, Linux, Mac OS.

⁵⁶ Mark Russinovich, autor szeregu narzędzi SYSINTERNALS, obecnie pracuje w firmie Microsoft

⁵⁷ http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal - obszerna informacja na temat przypadku wykorzystywania ROOTKITow przez firmę SONY

⁵⁸ ROOTKIT REVEALER - [http://technet.microsoft.com/pl-pl/sysinternals/bb897445\(en-us\).aspx](http://technet.microsoft.com/pl-pl/sysinternals/bb897445(en-us).aspx), autorstwa wspomnianego pana Marka Russinowicha

⁵⁹ SOPHOS ANTI-ROOTKIT - <http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html>

⁶⁰ GMER - <http://www.gmer.net/index.php>

4.8 Rejestr systemowy

Rejestr systemowy (ang. *System Registry*) – jest to hierarchiczna baza danych przechowywana w systemach Windows. W poprzednich wersjach systemów, ustawienia systemowe przechowywane były w plikach .ini a także w plikach autostartu. Rejestr systemowy pozwala nam na efektywne zarządzanie bieżącą konfiguracją ustawień komputera jak i również konfiguracją ustawień użytkownika. W oparciu o darmową bazę wiedzy Microsoft – Microsoft Technet⁶¹ oraz [Microsoft2], możemy określić strukturę i podstawowe elementy rejestru.

Rejestr składa się z hierarchicznej struktury podrzew i ich kluczy, podkluczy oraz wpisów. Musimy pamiętać, że zawartość rejestru danego komputera, może różnić się od zawartości innego komputera z uwagi na zainstalowane i uruchomione programy, usługi i sterowniki. Systemy Windows XP i Windows 2003 posiadają dwa poddrzewa: HKEY_LOCAL_MACHINE i HKEY_USERS. W celu ułatwienia przeglądania zawartości rejestru, narzędzia służące do przeglądania rejestru wyświetlają pięć podrzew, z czego trzy są aliasami do innych części rejestru. Pięć podstawowych podrzew rejestru przedstawiono w Tabeli 4.8.1.

Tabela 4.8.1 Struktura Rejestru (źródło witryna Microsoft Technet - <http://technet.microsoft.com/pl-pl/library/cc776231.aspx>)

Nazwa klucza głównego	Opis
HKEY_LOCAL_MACHINE	Zawiera informacje o systemie komputera lokalnego, włączając w to dane dotyczące sprzętu i systemu operacyjnego, takie jak typ magistrali, pamięć systemowa, sterowniki urządzeń i dane kontroli uruchamiania.
HKEY_CLASSES_ROOT	Zawiera informacje wykorzystywane przez różnego rodzaju technologie OLE i dane skojarzeń klas plików. Dany klucz lub wartość występuje w kluczu HKEY_CLASSES_ROOT , jeśli odpowiadający mu klucz lub wartość występuje w kluczu HKEY_LOCAL_MACHINE\SOFTWARE\Classes bądź kluczu HKEY_CURRENT_USER\SOFTWARE\Classes . Jeżeli klucz lub wartość występuje w obydwu miejscach, to wersja HKEY_CURRENT_USER jest tą, która występuje w kluczu HKEY_CLASSES_ROOT .
HKEY_CURRENT_USER	Zawiera profil użytkownika, który jest aktualnie zalogowany interaktywnie (jako przeciwieństwo zalogowania zdalnego), w tym zmienne środowiskowe, ustawienia pulpitu, połączenia sieciowe, drukarki i preferencje programów. To poddrzewo jest aliasem poddrzewa HKEY_USERS i wskazuje na HKEY_USERS\identyfikator_zabezpieczeń_bieżącego_użytkownika .

⁶¹ Opis Struktury Rejestru w Windows 2003 - <http://technet.microsoft.com/pl-pl/library/cc776231.aspx>

HKEY_USERS	Zawiera informacje o aktualnie załadowanych profilach użytkowników i profilu domyślnym. Część tych informacji pojawia się także w kluczu HKEY_CURRENT_USER . Użytkownicy uzyskujący zdalny dostęp do serwera nie mają profili pod tym kluczem na serwerze; ich profile są załadowane do rejestru ich własnych komputerów.
HKEY_CURRENT_CONFIG	Zawiera informacje o profilu sprzętowym używanym podczas uruchamiania komputera lokalnego. Te informacje są używane między innymi do konfiguracji ustawień, takich jak sterowniki urządzeń do załadowania i dostępne rozdzielczości wyświetlania. To poddrzewo wchodzi w skład poddrzewa HKEY_LOCAL_MACHINE i wskazuje klucz HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current .

W przypadku rejestru, musimy wprowadzić pojęcie „gałąź”, które określa grupę kluczy, podkluczy i wartości znajdujących się na szczycie hierarchii rejestru. Gałąź występuje w postaci pliku i pliku typu log, które znajdują się w folderach (zakładając, że system został zainstalowany w domyślnej lokalizacji **c:\windows**):

`C:\Windows\System32\Config` lub `c:\Documents and Settings\%Username`.

W domyślnej konfiguracji nowej instalacji systemu pliki gałęzi (**DEFAULT, SAM, SECURITY, SOFTWARE** i **SYSTEM**) są przechowywane w folderze **C:\System32\Config**. W systemach Windows Server 2003/XP pliki `Ntuser.dat` i `Ntuser.dat.log` są przechowywane w folderze **C:\Documents and Settings\%Username**.

Gałąź w rejestrze systemu Windows Server 2003/XP jest skojarzona ze zbiorem domyślnych plików. W Tabeli 4.8.2 zestawiono standardowe gałęzie i pliki.

Tabela 4.8.2 Struktura Rejestru – źródło witryna Microsoft Technet – <http://technet.microsoft.com/pl-pl/library/cc776231.aspx>

Gałąź rejestru	Nazwy plików
HKEY_LOCAL_MACHINE\SAM	Sam i Sam.log
HKEY_LOCAL_MACHINE\SECURITY	Security i Security.log
HKEY_LOCAL_MACHINE\SOFTWARE	Software i Software.log
HKEY_LOCAL_MACHINE\SYSTEM	System i System.log
HKEY_CURRENT_CONFIG	System i System.log
HKEY_CURRENT_USER	Ntuser.dat i Ntuser.dat.log
HKEY_USERS\DEFAULT	Default i Default.log

Podstawowym narzędziem służącym, do edycji, zmiany kluczy i wartości, eksportu i importu ustawień oraz wykonywania i przywracania kopii rejestru jest wbudowany program **REGEDIT**. W przypadku zaawansowanych programów do przeszukiwania i poszukiwania śladów w rejestrze systemowym, jako przykładowe komercyjne aplikacje

można wskazać pakiety **Paraben's Registry Analyzer**⁶², **ENCASE** oraz **Access Data Registry Viewer**. Na rynku darmowego oprogramowania dostępny był rewelacyjny program **Windows Registry Analyzer (WRA)**, ale od czasu przejścia praw do tego programu przez firmę PARABEN nie jest już dostępny w wersji darmowej, można natomiast skorzystać z wersji demonstracyjnej.

4.9 Odzyskiwanie skasowanych plików

Usuwanie plików z dysku jest jednym z elementów zacierania śladów. Polecenia usuwania plików zazwyczaj fizycznie nie kasują plików, tylko przenoszą je do odpowiedniego folderu, zwanego koszem. W przypadku usunięcia plików bez mechanizmu kosza, klastry w których znajduje się zawartość plików oznaczane są jak skasowane bez usuwania ich zawartości. Dane, które pozostają w klastrach znajdują się tam do czasu nadpisania ich poprzez inne pliki. Musimy tutaj pamiętać, iż mimo, że nazwa skasowanego pliku jest tracona, to jego zawartość pozostaje i może być odzyskana poprzez specjalne programy. Proces formatowania dysku i przygotowania go do pracy w systemie Windows, również nie usuwa zawartości danych w klastrach. Z perspektywy śledczych oznacza to, że pliki z dysków sformatowanych możliwe są do odtworzenia. Ponieważ w obecnych czasach dane zawarte na dyskach wielokrotnie przewyższają wartość samego dysku, rozwinęła się sfera profesjonalnych usług odzyskiwania danych. Specjalistyczne laboratoria podejmują się odzyskania nawet częściowych danych z urządzeń fizycznych, które zostały uszkodzone przez zalanie, zwarcie elektryczne czy częściowo niedziałającą część elektroniki urządzeń. W takich urządzeniach cały czas pozostają dane zapisane na nośnikach magnetycznych lub elektronicznych.

Kosz

Kosz (ang. Recycle Bin) – jest to specjalny folder w systemie Windows, w którym są umieszczone usunięte przez użytkownika pliki, np. poprzez naciśnięcie klawisza DEL w Windows Explorer. Główną funkcją kosza jest umożliwienie użytkownikowi przywrócenia pliku, który przypadkowo został usunięty. Wystarczy otworzyć folder kosz, znaleźć tam

⁶² Więcej informacji na witrynie producenta <http://www.paraben.com/>, oraz wersję DEMO, można jeszcze pobrać z witryny http://download.cnet.com/Paraben-s-Registry-Analyzer/3000-2092_4-10455699.html

usunięty plik, kliknąć prawym przyciskiem myszki i wybrać opcję przywróć plik. Lokalizacja kosza i jego struktura zależy od wersji systemu.

Tabela 4.9.1 Lokalizacja usuniętych plików w systemach Windows – źródło <http://www.forensicfocus.com/downloads/forensic-analysis-vista-recycle-bin.pdf>

System operacyjny	System plików	Lokalizacja usuniętych plików
Windows 95/98/ME	FAT32	C:\Recycled\INFO2
Windows NT/2K/XP	NTFS	C:\Recycler\<USER SID>\INFO2
Windows Vista	NTFS	C:\\$Recycle.Bin\<USER SID>\

W przypadku systemu Windows XP pliki znajdujące się w koszu otrzymują specyficzne nazwy tworzone wg schematu:

D[Litera dysku pliku][numer indeksu].[oryginalne rozszerzenie pliku]

Przykładowo dla usuniętego pliku c:\mojfolder\dokument1.doc, wpis będzie wyglądał następująco: **DC1.doc**, gdzie D – oznacza skasowany plik, C – literę dysku, z którego usunięto plik, 1 - numer indeksu. Indeks przy każdym skasowanym pliku zwiększa się o 1, przy czym numerowanie dla Systemu Windows XP/2003 zaczyna się od 1, w poprzednich wersjach, indeks rozpoczynał się od zera.

Jeśli przeglądamy z poziomu użytkownika zawartość kosza to widzimy nazwy oryginalnych plików, a to dzięki dodatkowemu plikowi **INFO2** (baza danych zawierająca informacje o plikach przechowywanych w koszu), w którym system Windows zapisuje takie informacje jak:

- Oryginalna nazwa pliku i ścieżka (przechowywana podwójnie, stosując system znaków ASCII i Unicode)
- Data i czas skasowania pliku
- Numer indeksu

W przypadku systemów Microsoft Vista i Windows 2008 usunięty plik zostanie przeniesiony do kosza i oryginalna nazwa zostanie zmieniona na „\$Rxxx.roz”, gdzie xxx to losowe liczby i cyfry a „roz” rozszerzenie identyczne jak w przypadku skasowanego pliku. Dodatkowo zamiast wpisu w pliku INFO2, tak jak to miało miejsce w poprzednim systemie, zostaje tworzony drugi plik „\$Ixxx.roz, w którym znajdują się informacje na temat skasowanego pliku:

- oryginalna nazwa usuniętego pliku
- rozmiar oryginalnego pliku
- data i czas usunięcia oryginalnego pliku.

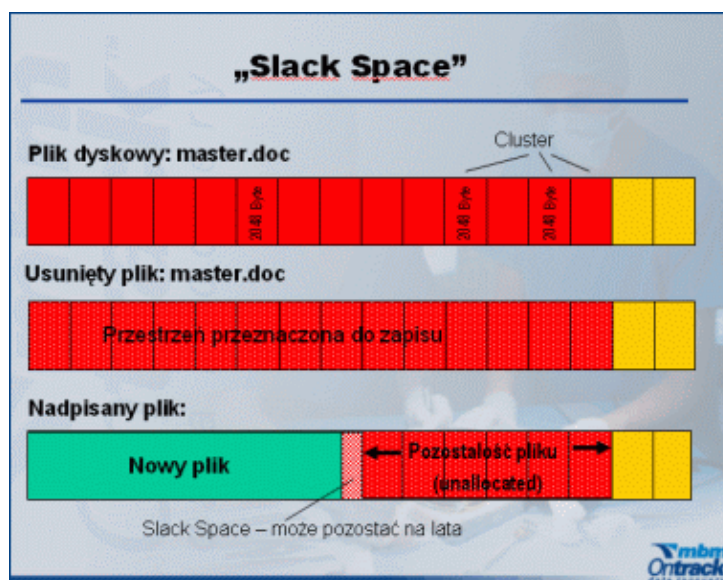
Więcej na temat różnic pomiędzy plikiem INFO2 a I\$ można znaleźć w dokumencie⁶³ lub dokumentacji systemu Windows Vista. Przykładowa para plików, która zawiera usunięty plik oraz informacje na temat usuniętego pliku może wyglądać tak:

\$IUD10V0.doc

\$RUD10V0.doc.

Obszary slack space

Slack space – są to resztki niewykorzystanych klastrów zawierające dane. Klaster jest to jednostka alokacji w systemie plików NTFS. Jeśli rozmiar danych jest mniejszy niż klaster, pozostaje obszar niezdefiniowany, w którym mogą się znajdować pozostałości poprzedniego pliku. Przykład opisujący tę sytuację przedstawiono na rysunku 4.9.2:



Rys. 4.9.2 – Lokalizacja danych w „Slack space”, źródło <http://www.krollontrack.pl/gfx/technonews/6.gif>, <http://www.krollontrack.pl/technonews,4.html>

Skuteczne usuwanie pliku

Opisane zachowanie systemu w przypadku usuwania plików jest powszechnie znane. Powstało wiele aplikacji, zarówno darmowych jak i komercyjnych, które pozwalają bezpiecznie skasować dane, poprzez kilkakrotnie nadpisywanie usuwanego pliku, w taki sposób, że śledczy nie znajdzie dowodów. Musimy tutaj pamiętać, że nie tylko my nie

⁶³ Mitchell Machor- “The Forensic Analysis of the Microsoft Windows Vista Recycle Bin” <http://www.forensicfocus.com/downloads/forensic-analysis-vista-recycle-bin.pdf>

będziemy w stanie odtworzyć w taki sposób wykasowanego pliku czy dysku, ale również profesjonalne firmy zajmujące się odtwarzaniem danych.

4.10 Użytkownicy i hasła

Komputer, którego badanie mamy przeprowadzić może być zabezpieczony hasłem. Hasło jest prywatną informacją, który każdy użytkownik chroni i nie jest ona dostępna dla innych osób. Użytkownik chcąc rozpocząć pracę musi podać swój login i hasło. Login jest swojego rodzaju kluczem, który wskazuje, które hasło system będzie sprawdzał.

Sposób uzyskania loginu i hasła zależy od tego jak dany komputer jest skonfigurowany. Możliwe są dwa podejścia:

- Praca w domenie Windows – komputery są podłączone do sieci i wykorzystują do logowania centralną bazę danych usługi katalogowej (ang. *Active Directory*) lub inną usługę opartej o standard LDAP.
- Praca w trybie „Standalone” lub „WORKGROUP” – komputery pracują niezależnie, mogą być przyłączone do sieci, ale nie są podłączone do centralnej bazy danych.

W przypadku pracy komputerów w trybie niezależnym, możemy skorzystać z wielu darmowych narzędzi wspomagających odzyskanie hasła, wykorzystujących ataki słownikowe lub typu siłowego (przeszukiwane są wszystkie możliwe hasła). Przykładem takiego narzędzia jest darmowy program LiveCD Ophcrack⁶⁴, który zawiera bootowalną płytę CD. Po uruchomieniu systemu z płyty CD możemy spróbować odczytać hasła z systemów Windows XP lub Vista. Ophcrack wykorzystuje tzw. „tęczowe tablice” (czyli bazę skrótów), co pozwala efektywnie korzystać z metody siłowej. Musimy jednak pamiętać, że jeśli hasło jest długie i skomplikowane poszukiwanie może trwać bardzo długo, lub może się nie udać w skończonym czasie.

W przypadku domeny, może okazać się, że nie będziemy w stanie odczytać hasła, ponieważ dane te są przechowywane w usłudze katalogowej. Wtedy możemy zwrócić się o pomoc do Administratora domeny.

4.11 Dane zaszyfrowane

Szyfrowanie danych przez użytkownika pozwala zabezpieczyć dane przed dostępem niepowołanych osób i zachować prywatność. W systemach Windows użytkownicy mogą

⁶⁴ LiveCD Ophcrack <http://ophcrack.sourceforge.net/>

skorzystać z wbudowanej funkcjonalności systemu NTFS, jaką jest szyfrowanie plików i katalogów. Technologia EFS (ang. *Encrypted File System*) pozwala na szyfrowanie i deszyfrowanie danych w locie, co oznacza w praktyce, że użytkownik może włączyć tę funkcjonalność i korzystać z niej bez zewnętrznych narzędzi. EFS oczywiście ma swoje wady. Słabością systemów Windows XP/2003 stosujących EFS jest przetrzymywanie klucza szyfrującego na tym samym dysku, na którym przechowane są zaszyfrowane dane. W przypadku nowszych systemów Windows 2008/Vista, możemy przechowywać certyfikaty wykorzystane przy EFS np. na kartach elektronicznych (ang. *SmartCard*) lub skorzystać z nowszej technologii BitLocker.

Deszyfrowanie danych wymaga posiadania klucza. Jeśli jest on niedostępny w przypadku EFS możemy skorzystać z programów do odzyskiwania kluczy szyfrujących, np. z komercyjnej aplikacji Advanced EFS Data Recovery firmy ELCOMSOFT⁶⁵ lub w przypadku poprawnie skonfigurowanego i wdrożonego rozwiązania EFS w domenie AD, z agenta odzyskiwania systemu szyfrowania plików (ang. *Recovery Agent*), który po zaimportowaniu certyfikatu pozwoli nam odszyfrować dane zaszyfrowane przez użytkownika domeny Windows.

EFS jest wbudowaną funkcjonalnością systemu NTFS w Windows. Na rynku możemy spotkać wiele komercyjnych aplikacji do szyfrowania zarówno plików, katalogów jak i całych dysków. Przykładem bardzo dobrej i darmowej aplikacji do szyfrowania całych dysków jest aplikacja TrueCrypt⁶⁶, w tym wypadku odtworzenie zaszyfrowanego dysku już nie jest takie proste, ale nie niemożliwe. Odszyfrowanie może wymagać dużo czasu i komercyjnych aplikacji do łamania i odzyskania hasła, którym zostały zaszyfrowane dane.

4.12 Logi systemowe i ich analiza

System Windows tworzy wiele logów – plików zawierających informacje, o tym co się zdarzyło w systemie bądź towarzyszyło zdarzeniom, programom lub usługom systemu Windows. Z punktu widzenia analizy znajdziemy w logach wiele przydatnych i interesujących informacji. Informacje zgromadzone w logach, mogą zawierać dane dotyczące instalacji, działania lub wykonywania poszczególnych elementów systemów

⁶⁵ Advanced EFS Data Recovery - <http://www.elcomsoft.com/aeafsdr.html>

⁶⁶ TrueCrypt - <http://www.truecrypt.org/>

Windows. Zdarzenia zarejestrowane mogą być wykonane przez system a także przez samych użytkowników.

Bieżące ustawienia dotyczące konfiguracji i informacji takich jak rozmiar czy sposób zarządzania logami (podczas przepełnienia plików logów) znajdziemy w kluczu rejestru systemowego:

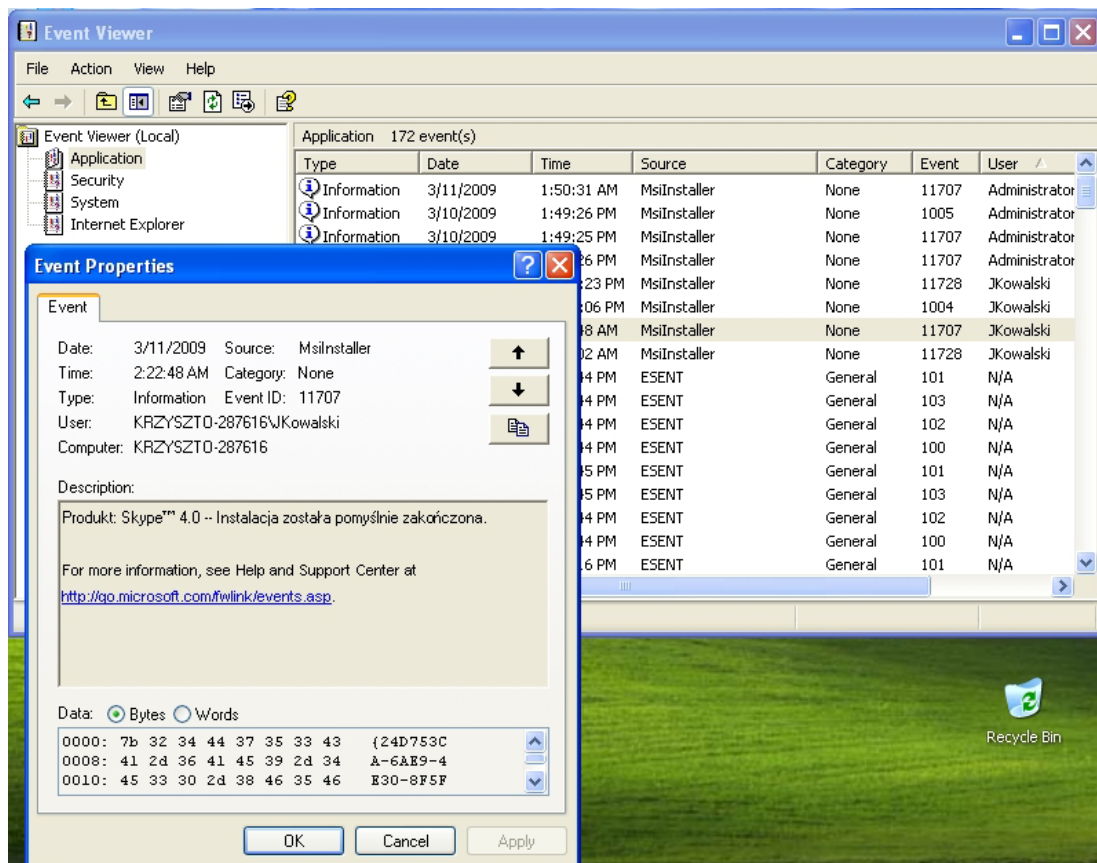
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\
```

Do zarządzania, filtrowania, eksportowania i odczytu zawartości systemowych logów służy wbudowane graficzne narzędzie „Podgląd Zdarzeń” (ang. *Event Viewer*), które pozwala nam na zarządzanie lokalnymi logami a także logami zgromadzonymi w innych systemach.

Każde zdarzenie zgromadzone w logach zawiera szczegółowe informacje takie jak:

- Data
- Czas
- Typ zdarzenia
- EventID: identyfikator zdarzenia
- Użytkownik
- Komputer
- Opis zdarzenia.

Przykładowy podgląd z analizowanego komputera podczas prowadzonych badań, przedstawia rysunek 4.12.1.



Rysunek 4.12.1 – Podgląd zdarzenia systemowego za pomocą narzędzia Event Viewer

Logi systemowe podzielone są na kategorie. Trzy główne kategorie logów w systemach Windows to:

- Zabezpieczenia (ang. *Security*)
- System (ang. *System*)
- Aplikacja (ang. *Application*)

W przypadku analizy zdarzeń zachodzących w naszym systemie, może okazać się bardzo pomocna witryna EventID.Net⁶⁷, gdzie znajdziemy dokładny opis około 10 000 zdarzeń.

Dodatkowe kategorie logów mogą pojawić się w systemie, po zainstalowaniu dodatkowych usług lub aplikacji np. Internet Explorer, MS Office. Zestaw logów jest związany również z tym, jakie funkcje pełni dana maszyna, mogą to być na przykład logi dotyczące serwera DNS lub usług katalogowych (Directory Services), które pojawią się na kontrolerze domenowym.

⁶⁷ EventID.Net - <http://www.eventid.net/>

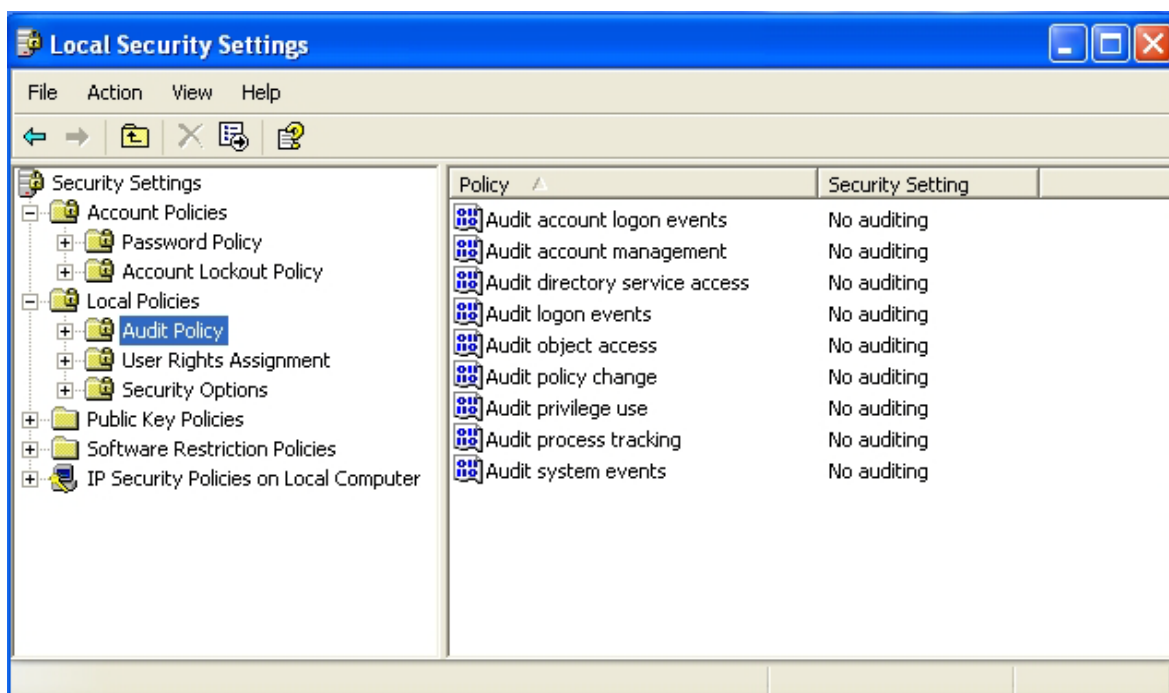
W przypadku nowszych systemów takich jak Windows Vista czy Windows 2008, logi zostało podzielone na wiele podkategorii, ułatwiając tym samym analizę pod kątem działających funkcjonalności czy usług.

Logi w systemach Windows XP/2003 posiadają rozszerzenie **.evt**, i mogą być wyeksportowane do formatu tekstowego lub bazy danych SQL. Logi w nowszych systemach Windows Vista i 2008 posiadają rozszerzenie **.evtx** i są przechowywane są w formacie XML.

Analizując logi musimy pamiętać o inspekcji zdarzeń (ang. *Audit Policy*), która określa zakres zbieranej informacji. Możliwe opcje do ustawienia to:

- Brak inspekcji (ang. *No Auditing*)
- Sukces (ang. *Audit Successes*)
- Niepowodzenie (ang. *Audit Failures*)
- Sukces i Niepowodzenie (ang. *Audit Success and Failures*)

Domyślnie system Windows ma wyłączoną inspekcję zdarzeń, co pokazuje rysunek 4.12.2



Rysunek 4.12.2 – Domyślne ustawienia polityki inspekcji zdarzeń

Dodatkową analizę logów może ułatwić darmowy program wydany przez firmę Microsoft **Log Parser**⁶⁸ oraz wiele innych komercyjnych aplikacji automatyzujących przetwarzanie i zarządzanie procesem zbierania i analizy logów.

Podczas analizy logów nie możemy zapomnieć również o plikach tekstowych, w których znajduje się wiele cennych informacji, np. Setuplog.txt, Setupact.log, SetupApi.log, Netsetup.log, Schedlgu.txt czy wiele, wiele innych. Pełną listę plików logów znajdziemy w opracowaniu **Microsoft Windows Server 2003 Resource Kit**⁶⁹.

Musimy tutaj pamiętać o szczegółowych logach innych aplikacji czy produktów zewnętrznych takich jak:

- IIS Server – serwer WWW i ftp,
- SQL Server – serwer bazy danych,

które zarządzają i gromadzą logi według własnych ustawień.

W zasadzie każdy z dodatkowych programów zainstalowanych w naszym systemie, może zarządzać i tworzyć logi w sposób charakterystyczny dla danej aplikacji, co wymaga zapoznania się z odpowiednią dokumentacją techniczną.

⁶⁸ Log Parser v.2.2 - <http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx>


⁶⁹ Biblioteka techniczna systemu Windows Server 2003 - <http://technet.microsoft.com/pl-pl/library/cc706993.aspx>

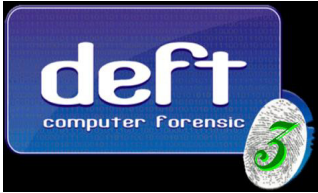
5. PRZEGLĄD NARZĘDZI STOSOWANYCH

W INFORMATYCE ŚLEDZCZEJ


W poprzednich rozdziałach przedstawiono różne polecenia, które mogą być użyteczne podczas prowadzonego śledztwa. Niektóre z nich wchodziły w skład poleceń systemowych, inne wymagają zainstalowania odpowiedniego pakietu programów. Wygodniej byłoby zorganizować je w postaci gotowych zestawów. I rzeczywiście takie zestawy są udostępniane. Poniżej omówiono te najbardziej popularne, zarówno darmowe jak i komercyjne. W pracy wykorzystano jedno z omawianych narzędzi o nazwie Helix.

5.1 Przegląd darmowych zestawów narzędzi


Nazwa:	HELIX Live CD	
Wersja:	HELIX 1.9a (07-13-2007)	
Producent:	e-fense inc.	
Adres URL:	http://www.e-fense.com/helix/index.php	
Środowisko:	Windows/Linux	
Typ:	BOOT CD	
Licencja	Darmowa	
<p>Jedna z najlepszych dystrybucji narzędzi zgromadzonych na jednej płycie CD. Narzędzia działają zarówno pod system Linux jak i Windows. Większość omawianych pojedynczych programów i aplikacji opisanych w poprzednich rozdziałach znajduje się właśnie na tej płycie. Wystarczy po prostu z nich skorzystać. Pakiet Helix jako jeden z nielicznych, pozwala na podłączenie wolumenów i dysków w sposób niepozostawiający śladów i modyfikacji w badanym systemie. Początkujący, oprócz przygotowanego zestawu programów w bardzo przejrzysty i prosty sposób znajdą również ponad 300 stronicową dokumentację, która dokładnie opisuje zgromadzone programy a także zawiera materiały pozwalające na zapoznanie się z technikami Informatyki śledczej. O popularności pakietu, może świadczyć fakt prowadzenia komercyjnych szkoleń z dziedziny informatyki śledczej, bazujących właśnie na pakiecie HELIX. W chwili obecnej aplikacja nie jest już dostępna za darmo, ale poprzez płatny abonament. W sieci można jeszcze znaleźć obraz ISO darmowego narzędzia - Helix_V1.9-07-13a-2007.iso.</p>		

Nazwa:	deft compute forensic	
Wersja:	deftv401x.iso	
Producent/Autor:	dr. Stefano Fratepietro dr. Massimiliano Dal Cero	
Adres URL:	http://deft.yourside.it/	
Środowisko:	Xubuntu live Linux CD	
Typ:	BOOT LIVE CD (format .iso)	
Licencja	Free and Open Source Software	


Zestaw stworzony z myślą o analizie sprzętowej i zarządzaniu incydemem a także analizie powłamiowej. Przeznaczony dla policji, śledczych lub administratorów. Zestaw ten dodatkowo zawiera wersję, którą można uruchamiać z urządzenia Pendrive. W skład pakietu wchodzi popularne narzędzia Sleuthkit czy Autopsy, ale także narzędzia służące do łamania haseł, wykrywania stegnaografii czy wykonywania kopii bitowej. Na płycie znajdują się również narzędzia do wykrywania rootkitów oraz programy do odtwarzania skasowanych plików.

Nazwa:	FCCU Gnu/Linux boot CD	
Wersja:	fccu-linux-cd-12.0.iso	
Autorzy:	lnx4n6.be - The Belgian Computer Forensic, autorzy :Christophe Monniez (d-fence) oraz Geert Van Acker	
Adres URL:	http://www.lnx4n6.be/	
Środowisko:	KNOPPIX Live CD version 4.02	
Typ:	BOOT LIVE CD	
Licencja	Darmowa	


Darmowe narzędzie oparte na darmowych rozwiązaniach bazujących na systemie KNOPIIX Live CD. Zestaw stworzony przez zespół Belgian Federal Computer Crime Unit (FCCU), z myślą o pomaganiu innym przy analizie i badaniu podejrzanych komputerów. Narzędzia zgromadzone w tym zestawie są podzielone na kilka kategorii. Jednym z ciekawszych są narzędzia łamiące hasła w plikach zip czy danych zaszyfrowanych przy pomocy PGP.

Nazwa:	The Penguin Sleuth Kit	
Wersja:	penguinsleuth-07-05-2003.iso v 1.1	
Producent/Autor:	Ernest Baca	
Adres URL:	http://penguinsleuth.org/	
Środowisko:	Knoppix Linux	
Typ:	BOOT LIVE CD (format .iso)	
Licencja		

Pakiet przygotowany w postaci Linux Live CD, zawierający zestaw narzędzi do analizy w postaci poleceń tekstowych. Może być przydatny do analizy systemów plików FAT, NTFS i innych, odzyskiwania usuniętych plików. Penguin Sleuth Kit, który pozwala nam dokonać analizy wykorzystując nie tylko przygotowany zestaw narzędzi ale przygotowany z myślą o własnoręcznym dodawaniu własnych narzędzi i programów lub dostosować pakiet do własnych potrzeb.


Nazwa:	Back Track 3 / 4 Beta	
Wersja:	bt3-final.iso / bt4-beta.iso – DVD Image	
Producent/Autor:	Zespół specjalistów pod nazwą Remote-Exploit	
Adres URL:	http://www.remote-exploit.org/backtrack.html	
Środowisko:	live Linux CD/DVD/HDD/Pendrive	
Typ:	BOOT LIVE CD/DVD (format .iso)	
Licencja	Free and Open Source Software	

Zestaw narzędzi oparty na dystrybucji Slax. Powstał w wyniku połączenia systemów do penetracji Whax i Auditor. Zawiera głównie oprogramowanie, które służy do testów bezpieczeństwa, łamania zabezpieczeń i testów penetracyjnych. System można uruchomić z dysku twardego, płyty C/DVD oraz pendrive USB. W chwili obecnej dostępna jest beta 4 wersji systemu. Jest to kompletny zestaw, którego głównym odbiorcami są audytorzy lub osoby badające stan bezpieczeństwa. Zestaw ten zawiera narzędzia z zakresu: zbierania informacji wewnątrz sieci, penetracji, łamania haseł, badania podatności urządzeń Cisco, baz danych czy serwerów WWW. Wśród narzędzi znajdują się również snifery i programy do analizy sieci bezprzewodowych.

Nazwa:	Knoppix STD 0.1	
Wersja:	knoppix-std-0.1.iso	
Producent/Autor:	S-T-D Staff	
Adres URL:	http://s-t-d.org/	
Środowisko:	Knoppix Linux	
Typ:	BOOT LIVE CD (format .iso)	
Licencja	GPL / open source	

Zestaw programów w postaci systemu gotowego do użycia, po uruchomieniu z płyty CD. Na tym systemie bazuje wiele dystrybucji innych pakietów do Informatyki śledczej. Zaletą tego pakietu jest możliwość wykorzystania go do zbudowania serwera bez instalacji, który będzie świadczył usługi współdzielenia plików czy przygotowania i zestawienia bezpiecznych tuneli do zbierania i przechowywania logów i plików podczas wykonywanej analizy. W zestawie narzędzia zostały podzielone na kategorie: informatyka śledcza, szyfrowanie, IDS, honeypots, narzędzia sieciowe oraz testy badające podatność systemów. Główną zaletą tego pakietu są narzędzia sieciowe, które pozwalają na analizę online incydentu, który właśnie trwa i naszym zadaniem jest zabezpieczenie jak największej ilości śladów ruchu sieciowego.

5.2 Przegląd komercyjnych zestawów narzędzi

Nazwa:	Zestaw produktów EnCase	
Producent/Autor:	Guidance Software	
Adres URL:	http://www.encase.com/	
Środowisko:	Linux, Windows	

Bardzo zaawansowany zestaw produktów. Encase to zestaw produktów wspomagających pracę śledczych lub firm świadczących usługi komercyjne. Może być przydatny zarówno pojedynczym użytkownikom, jak i całym zespołom gdyż umożliwia pracę grupową nad danym incydem. W zestawie znajduje się wiele narzędzi wspomagających automatyczną analizę i wyszukiwanie śladów. Potężne narzędzie z dobrym zapleczem edukacyjnym w postaci kursów, egzaminów i książek [EnCase]. Obrazy i raporty wykonane za pomocą tego produktu są honorowane w sądach na całym świecie, a także sam format dowodu elektronicznego jest rozpoznawalny i akceptowalny w środowisku Informatyki śledczej.

Najnowsza wersja EnCase Forensic version 6, wspiera sprzętowe blokery. Aplikacja ta pozwala na zbieranie danych w sposób umożliwiający przedstawienie ich w sądzie. Pakiet ten obsługuje wiele systemów takich jak Windows, Linux oraz AiX, OS X, Palm, Macintosh czy Solaris oraz wiele innych. EnCase pozwala w łatwy sposób zarządzać wolumenami z danymi oraz wspomaga analizę charakterystycznych miejsc systemów operacyjnych wraz z odtwarzaniem i analizą usuniętych plików, „slack space” czy nie przydzielonych miejsc danych.

Obsługuje i konwertuje większość znanych formatów obrazów kopii bitowej zebranych dowodów, pozwala na wykorzystanie kompresji w zgromadzonych plikach obrazów.


Jak potężny to jest pakiet, może świadczyć obsługa takich funkcjonalności:

- obsługa szyfrowanych dysków
- wsparcie dla międzynarodowych formatów kodowania znaków
- analizator bazy Active Directory zawartej w pliku NTDS.DIT, który pozwala na wyciągnięcie informacji na temat nazw kont, identyfikatorów SID, czy inne właściwości obiektów AD
- automatyczna analiza i przeszukanie plików logów i zdarzeń systemowych
- wbudowany edytor rejestru
- obsługa meta danych różnych systemów plików
- obsługa popularnych formatów plików poczty elektronicznej
- przeglądania i analiza przeglądanych witryn internetowych .

Raporty – pakiet ten pozwala na automatyczne tworzenie raportów, szczegółowość raportów zależy od grupy docelowej, jaką wybierzemy podczas przygotowywania raportu. Przedstawiane dane w sposób dedykowany dla odbiorców raportów, od bardzo szczegółowego raportu technicznego do minimalnego przeznaczonego dla ławy przysięgłej.

Mocną stroną tego pakietu jest możliwość tworzenia zapytań i przeszukiwania danych pod kątem przygotowanego zapytania. Za pomocą wbudowanego języka skryptów EnScript, możemy sami napisać skrypty przeszukujące dane jeśli przygotowane funkcjonalności nam nie wystarczą.


Interfejs graficzny jest na tyle łatwy i intuicyjny, że nawet osoby nie związane z informatyką np. adwokaci, którzy muszą się zapoznać z zebranymi dowodami, mogą to zrobić z łatwością.

Nazwa:	Forensics Software, Forensics Hardware	
Producent/Autor:	PARABEN CORPORATION	
Adres URL:	http://www.paraben.com/	
Środowisko:	Linux, Windows, hardware	


Forensics Software to wiele produktów zgrupowanych w kilka podkategorii, takich jak analiza telefonów komórkowych, emaili czy bardzo zaawansowany edytor rejestru. W zestawie znajduje się wiele narzędzi wspomagających automatyczną analizę i wyszukiwanie śladów. Producent zadbał również o zaplecze edukacyjne w postaci kursów, egzaminów i książek, które oprócz zaoferowanych produktów komercyjnych pozwalają na poszerzenie wiedzy i wykorzystywanie jej podczas prowadzonych badań. W ofercie firmy znajdziemy również urządzenia sprzętowe wspomagające pracę śledczych, takie jak blokery czy zestawy do podłączania telefonów komórkowych. Są to gotowe zestawy, które pomagają śledczym, który przybyli na miejsce w celu zebrania i zabezpieczenia dowodów elektronicznych.

Nazwa:	WinHex , X-Ways Forensics, Investigator,	
Producent/Autor:	X-Ways Software Technology AG	
Adres URL:	http://www.sf-soft.de/	
Środowisko:	Linux, Windows,	

Firma X-Ways dostarczyła na rynek kilka produktów wspomagających analizę. Między innymi edytor WinHex, który pozwala na edycję i analizę dysku i pamięci RAM. Edytor ten uważany jest za jeden z najlepszych produktów wspomagających zaawansowaną analizę dysków czy zawartości pamięci RAM.

Nazwa:	Forensic Toolkit	
Producent/Autor:	AccessData	
Adres URL:	http://www.accessdata.com/	
Środowisko:	Linux, Windows,	

Rodzina komercyjnych programów do analizy śledczej. Pozwalają na analizę rejestru, deszyfrowanie plików, łamanie haseł czy identyfikację steganografii. Wspomaga proces przeszukiwania i poszukiwania śladów oraz złożony proces raportowania. Na wyróżnienie zasługuje wspomaganie pracy grupowej przy tworzonej analizie, pozwalający na pracę grupie osób przy trudnych i długotrwałych incydentach. Na szczególną uwagę zasługują narzędzie „DNS – Distributed Network Attack” wspomagające łamanie haseł przy pomocy nie tylko jednego komputera ale wykorzystanie mocy wielu komputerów połączonych w sieci, co w znacznym stopniu przyspiesza uzyskanie oczekiwanych efektów.

Nazwa:	ProDiscover Family	
Producent/Autor:	Technology Pathways	
Adres URL:	http://www.techpathways.com/	
Środowisko:	Linux, Windows,	
<p>Oprogramowanie wspiera szybkie i wydajne śledztwa podczas działania systemów, bez przerywania pracy badanych komputerów i systemów. Pozwala na badanie i monitorowanie pod kątem zgodności z wewnętrznymi procedurami i zaleceniami. Pozwala na analizę między innymi plików pocztowych ale też wszelkich zagadnień związanych z zarządzaniem i monitorowaniem incydentów. Siłą tego rozwiązania jest wszechstronne wsparcie zbierania i analizowania danych znajdujących się na twardych dyskach przy pomocy agentów pozwalających na przesyłanie danych poprzez sieć bez zatrzymywania pracy komputerów.</p>		

6. ANALIZA PRZYPADKU

W tej części zajmiemy się praktyczną analizą przypadku, jaki możemy spotkać w wielu przedsiębiorstwach czy organizacjach związanego z ujawnieniem pewnych danych wewnętrznych firmy. Scenariusz jest tak zaprojektowany aby można było przedstawić narzędzia i sposób postępowania pozwalający wyjaśnić zdarzenia, które miały miejsce.

W obecnych czasach większość firm wyposaża swoich pracowników w komputer firmowy wraz z systemem Windows, który jest podstawowym narzędziem pracy. Oznacza to również, że pracownik dostaje narzędzie, za pomocą którego można dokonywać przestępstw komputerowych.

6.1 Scenariusz

Do celów badawczych, wykorzystano i przyjęto następujący scenariusz. Firma „COMPANY” zatrudnia pracownika Jana Kowalskiego pracującego na stanowisku specjalisty w dziale Marketingu. W polityce bezpieczeństwa firmy zawarto zapisy, które zabraniają pracownikom udostępniania bądź ujawniania tajemnicy przedsiębiorstwa w jakiegokolwiek formie. Pracownik Jan Kowalski, zapoznał się z obowiązującymi przepisami i podpisał osobiście akceptację wymienionych warunków.

Pan Kowalski przyjaźni się z Panem Andrzejem Nowakiem, pracownikiem firmy „FIRMA” zatrudnionym na stanowisku pracownika działu marketingu. Obaj Panowie utrzymują bliskie kontakty towarzyskie.

Zarząd firmy „COMPANY” zaniepokojony jest informacjami o przejęciu i wykorzystaniu planów marketingowych przez konkurencyjną firmę „FIRMA”. Zarząd podjął decyzję o zbadaniu szczegółowo sprawy. Po wstępnej analizie ustalono wspólne kontakty i potencjalne źródło przecieku, wskazano Pana Jana Kowalskiego, pracownika firmy „COMPANY” oraz pana Andrzeja Nowaka z firmy „FIRMA”. Przeprowadzono rozmowę z Panem Kowalskim, w której nie przyznał się do zarzucanych czynów.

Zarząd firmy „COMPANY” postanowił zlecić zbadanie śladów, które mogą znajdować się na komputerze pana Kowalskiego.

6.2 Opis przygotowanego środowiska testowego

Celem testów jest zbadanie komputera i ustalenie istnienia dowodów naruszenia polityki bezpieczeństwa – ujawnienie tajemnicy przedsiębiorstwa dokonane przez pana Jana Kowalskiego. Na potrzeby analizy przygotowano hipotetyczny komputer pana Kowalskiego. Jest to standardowy komputer biurowy wykorzystywany w codziennej pracy wraz z zainstalowanym systemem Microsoft Windows XP Professional. System Windows został zainstalowany w wirtualnej maszynie, wykorzystując technikę wirtualizacji. Technika ta emuluje pracę fizycznego komputera. Na komputerze skonfigurowano dostęp do Internetu, aplikację Microsoft Office Professional 2003 wraz z programem Outlook do obsługi poczty elektronicznej oraz komunikatory internetowe: Gadu-Gadu oraz SKYPE. Wykorzystane środowisko wirtualne to aplikacja VMware Workstation 6.5.1 build – 126130 w wersji testowej (30 dniowy okres próbny). Środowisko to w znacznym stopniu ułatwiło przeprowadzenie badań oraz wykorzystanie przygotowanych darmowych narzędzi w postaci obrazów ISO oraz zestawu niezbędnych programów wspomagających analizę.

Na komputerze pana Kowalskiego przygotowano ślady jego działalności związanej z ujawnieniem tajemnic przedsiębiorstwa.

Dodatkowo utworzono rzeczywiste konta darmowej poczty elektronicznej oraz konta użytkownika systemu GaduGadu oraz Skype umożliwiające komunikowanie się między panami Kowalskim i Nowakiem:

Osoba: Jan Kowalski jkowalski3456@wp.pl GaduGadu 8670993 Skype: jkowalski3456	Osoba: Andrzej Nowak anowak3456@wp.pl GaduGadu: 8731293 Skype: anowak3456
--	--

6.3 Analiza

Podczas analizy wykorzystano model analizy informatyki śledczej przedstawiony na rys.1.1. Zgodnie z nim analizę przeprowadzono w czterech etapach. Wszystkie pliki zgromadzone podczas analizy wraz z kopią bitową analizowanego komputera znajdują się na płycie DVD dołączonej do pracy magisterskiej.

6.3.1 Oszacowanie sytuacji

Na spotkaniu zarządu firmy „COMPANY” z Administratorem (w roli administratora występuje autor pracy – Krzysztof Bińkowski) przedyskutowano ewentualne możliwości i sposoby udostępnienia danych konkurencji przez pana Jana Kowalskiego. Możliwością było kilka, jedną z nich było wysłanie danych przez Internet, za pośrednictwem poczty elektronicznej lub komunikatora. Po konsultacjach z działem prawnym w aspekcie obowiązujących procedur w firmie, udzielono pisemnego zezwolenia na zabezpieczenie komputera Pana Jana Kowalskiego i wykonanie śledztwa wewnętrznego przez administratora Krzysztofa Bińkowskiego.

Administrator w pierwszej kolejności zidentyfikował podejrzany komputer. Komputer ten posiadał przypisaną nazwę: **KRZYSZTO-287616**, pracował w grupie roboczej WORKGROUP i był podłączony do infrastruktury sieci firmowej firmy „COMPANY”, komputer był uruchomiony.

6.3.2 Pozyskiwanie danych

Administrator działając w oparciu o wydane pisemne zezwolenie zdecydował się na wykonanie kopii bitowej dysku, oraz zabezpieczenie komputera poprzez zdeponowanie go w sejfie.

Wykonano kopię bitową dysku w ilości 2 szt., za pomocą programu **AccessData FTK Imager w wersji 2.5.3.14 Lite** (w przykładowym środowisku wszystkie narzędzia były uruchamiane z udostępnionego zasobu sieciowego). W wyniku powstały pliki:

- **komp_jk.dd.001** - 2,99 GB (3 220 955 136 bytes) – obraz dysku komputera
- **komp_jk.dd.001.txt** – informacje szczegółowe na temat badanego dysku
- obliczono funkcje skrótu dla wykonanego obrazu:
MD5 checksum: f813c6c709c1602b8145a1ddc2b7e99d
SHA1 checksum: 2ffef538eabb22226d622dd05c8ae0aa0fcc2db3
- **komp_jk.dd.001.csv** – wykaz wszystkich plików wykonany podczas tworzenia obrazu

Następnie komputer został wyłączony i zdeponowany w magazynie. Pominięto krok zbierania danych ulotnych, ponieważ założony scenariusz, nie zakładał takich śladów.

6.3.3 Analiza zgromadzonych danych

Analizę rozpoczęto od skonfigurowania i uruchomienia działającego systemu Microsoft Windows XP w środowisku wirtualnym VMware Workstation, bazującego na obrazie z pliku **komp_ik.dd.001**. Do tego celu użyto darmowego narzędzia **Live View 0.7b**⁷⁰ – które pozwala, przygotować konfigurację maszyny wirtualnej w środowisku VMWare na podstawie obrazu dysku w postaci formatu dd lub fizycznego dysku. Program pozwala na uruchomienie wirtualnej maszyny i pracę na niej, bez dokonywania modyfikacji podłączonego obrazu lub dysku fizycznego, wszelkie zmiany zapisywane są w oddzielnym pliku, co pozwala badającemu na uruchomienie za każdym razem, maszyny z oryginalnego, nie zmodyfikowanego obrazu dysku.

Zalogowano się do komputera wykorzystując to tego celu konto „Administrator”.

W pierwszym kroku zbadano czy są usunięte pliki, które mogą zostać odzyskane. Czynność tę wykonano za pomocą darmowego programu **RECUVA w wersji 1.24.399**⁷¹.

Odzyskane pliki zgromadzono w katalogu `\raport.mgr\recuva`, łącznie odzyskano 406 pliki.

Po analizie szczegółowej, uwagę zwrócono na dwa odzyskane pliki Excela:

- **[000147].xls - 33,5 KB (34 304 bytes)** – zawierający plany
- **[000002].xls - 44,7 KB (45 864 bytes)** – zawierający listę płac

Zawartość plików została odzyskana z sektorów jeszcze nie nadpisanych przez inne dane, co może świadczyć o tym, że pliki zostało celowo usunięte w ostatniej chwili, brak informacji na temat właściciela i znaczników czasu związanych z tymi plikami.

W kolejnym etapie poddano analizie dane związane z komunikatorami:

Komunikator GaduGadu

Do zbadania archiwum programu GaduGadu, użyto narzędzia **GGTols 2.6 release 3**⁷². Badany plik to `C:\Documents and Settings\JKowalski\GaduGadu\Ja\archives.dat`

Wyniki zapisano w pliku `\raport.mgr\gg\raport_gg.txt`

Analiza pliku wskazała na komunikację z Panem Andrzejem Nowakiem. Znaleziono również wskazówkę. Podany przez Pana Nowaka adres

⁷⁰ Live View 0.7b - <http://liveview.sourceforge.net/>

⁷¹ “RECUVA File Recovery” - <http://www.recuva.com/>

<http://www.brothersoft.com/trojan-image-security-50247.html> jest adresem, z którego można ściągnąć program **Trojan Image Security 1.0**, służący do ukrywania plików wewnątrz plików graficznych. Program ten został zainstalowany na badanym komputerze w dniu 12.03.2009.

Komunikator SKYPE

Do sprawdzenia archiwum SKYPE, znajdującego się w pliku C:\Documents and Settings\JKowalski\Application Data \Skype \jkwalski3456\main.db wykorzystano program **SkypeLogView v.1.10**⁷³. Plik logu został zapisany w \\raport.mgr\skype\skypelog.mht. Zbadanie pliku logów programu Skype nie wniosła nic nowego do analizy.

Analiza poczty elektronicznej zawartej w pliku pst

Do analizy znalezionej pliku C:\Documents and Settings\JKowalski\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst wykorzystano program Outlook, zainstalowany na badanym komputerze. Wykorzystano profil Administratora. Przy próbie otwarcia pliku, okazało się, że plik jest zabezpieczony hasłem. Do dalszej analizy niezbędne było odzyskanie hasła do pliku poczty. Do tego celu wykorzystano darmowy program **PstPassword v.1.12**⁷⁴. Korzystając z programu odzyskano kilka haseł, pozwalających na dostęp do badanego pliku poczty. Raport z odzyskanymi hasłami został zapisany w \\raport.mgr\outlook\PST Passwords List.mht. Przy pomocy odzyskanego hasła otworzono plik z pocztą Pana Jana Kowalskiego.

Po zbadaniu zawartych w pliku wiadomości, ustalono liczne dowody komunikacji pomiędzy Panami Janem Kowalskim i Andrzejem Nowakiem. Analiza pozwoliła ustalić, iż Jan Kowalski wysłał dwa emaile z załącznikami do Pana Andrzeja Nowaka. Szczegóły wykrytych wiadomości przedstawiono poniżej:

Od: Jan Kowalski [jkwalski3456@wp.pl]

Wysłano: Thursday, March 12, 2009 11:30 PM

Do: 'anowak3456@wp.pl'

Temat: obiecane foto bmw

Załącznik: bmw32.bmp

⁷² "GGTols 2.6 release 3", autor Krzysztof 'kRk' Mortka - <http://mortka.pl/>

⁷³ SkypeLogView - <http://www.nirsoft.net/> - http://www.nirsoft.net/utills/skype_log_view.html

Od: Jan Kowalski [jkowalski3456@wp.pl]
Wysłano: Thursday, March 12, 2009 11:28 PM
Do: 'anowak3456@wp.pl'
Temat: fajna tapeta
Załącznik: Sexy_Bikini_0362.bmp

Pliki załączników poddano dalszej analizie.

Analiza plików załączników

W pierwszej kolejności odszukano pliki wskazane w poczcie. Znaleziono pliki **bmw3.bmp** i **bmw32.bmp** w katalogu:

C:\Documents and Settings\JKowalski\My Documents\samochody
oraz **Sexy_Bikini_036.bmp** i **Sexy_Bikini_0362.bmp** w katalogu:

C:\Documents and Settings\JKowalski\My Documents\fotki

Identyczne co do wielkości pliki **bmw3.bmp** i **bmw32.bmp**, zostały przejrzane i wyświetlone za pomocą wbudowanego programu do przeglądania plików graficznych. Zmian wizualnych nie dostrzeżono.

W kolejnym kroku poddano pliki porównaniu binarnym za pomocą wbudowanego w systemie Windows programu **FC** (File Compare):

```
FC bmw3.bmp bmw32.bmp > wynik.txt
```

Porównanie plików pozwoliło stwierdzić, że pliki mają różną zawartość i mogą zawierać ukryte dane, pomimo identycznego rozmiaru plików.

W identyczny sposób porównano pliki **Sexy_Bikini_036.bmp** i **Sexy_Bikini_0362.bmp**. Pliki również miały różną zawartość i mogły zawierać ukryte dane.

Na badanym komputerze został znaleziony program „Trojan Image Security 1.0”. Jest to znane narzędzie służące do ukrywania plików w plikach graficznych. Za jego pomocą, otworzono i zbadano wysłane załączniki:

pliki - **bmw32.bmp** i **Sexy_Bikini_0362.bmp**

⁷⁴ PstPassword v.1.12 - http://www.nirsoft.net/utills/pst_password.html

Analiza wskazanych plików wykazała, iż w przesłanych plikach graficznych były ukryte pliki programu Excel zawierające poufne dane:

- Plik przedstawiający zdjęcie samochodu **bmw32.bmp** – zawierał arkusz kalkulacyjny: **Plan_fundusz.xls - 45,0 KB (46 080 bytes)**
- Plik z motywem tapety **Sexy_Bikini_0362.bmp** – zawierał arkusz kalkulacyjny **Lista_plac_2009_01.xls - 33,5 KB (34 304 bytes)**

Ukryte pliki oraz pliki, w których ukryto dane zostały umieszczone w katalogu
\raport.mgr\steganografia

Alternatywne strumienie danych

Komputer poddano analizie pod kątem ukrytych plików w alternatywnych strumieniach danych. Do analizy wykorzystano darmową aplikację **STREAMS v1.56⁷⁵**, Wynik poszukiwań został umieszczony w pliku \raport.mgr\ads\ads.txt.

Podejrzenie wzbudził znaleziony plik **zadania.txt** wewnątrz katalogu domowego użytkownika Jan Kowalskiego, który zawierał ukryty plik **moje.txt**:

```
c:\Documents and Settings\JKowalski\My Documents\zadania\zadania.txt:  
      :moje.txt:$DATA 165
```

Zawartość plików zbadano przy pomocy notatnika. Wykorzystano polecenie

```
Notepad zadania.txt  
Notepad zadania.txt:moje.txt
```

Następnie pliki wyeksportowano przy pomocy programu FTK Imager i umieszczono w katalogu \raport.mgr\ads

Plik **moje.txt** zawierał ukryte treści:

```
wyslac Andrzejowi fotki  
wyslac liste plac i plany  
upomniec sie o zaplata za ciezka prace ;)  
wyslac CV do Andrzeja  
Tel. do Andrzeja 500 500 xxx
```

Zabezpieczenia dowodów

⁷⁵ STREAMS - <http://technet.microsoft.com/en-us/sysinternals/bb897440.aspx>

Podczas procesu zbierania i analizowania danych dla każdego badanego pliku została utworzona suma kontrolna przy pomocy programu **FCIV**⁷⁶ stosując algorytm SHA1:

```
Fciv -add nazwa pliku -sha1 > nazwa pliku.sha1
```

6.3.4 Przygotowanie raportu:

Zabrane dowody posłużyły do przygotowania raportu. Ustalono, że będzie on zawierał następujące sekcje:

- Cel raportu
- Autor raportu
- Podsumowanie incydentu
- Informacja na temat zabezpieczonego dysku jako dowodu
- Opis procesu analizy oraz znalezionych dowodów
- Wnioski
- Lista plików stanowiących załączniki

Raport został przedstawiony w Załączniku 2 oraz w postaci pliku na dołączonej płycie DVD. Do przygotowania raportu wykorzystano darmowy szablon „**Forensic Investigation Report Template**” autorstwa Rnewhall⁷⁷, który obejmuje przykładowe sekcje oraz wykaz niezbędnych informacji, które muszą się znaleźć w raporcie.

6.4. Wnioski

Na badanym komputerze znaleziono liczne ślady komunikacji pomiędzy podejrzanym osobami Panem Janem Kowalskim a Panem Andrzejem Nowakiem. Pan Jan Kowalski był w stałym kontakcie z Panem Andrzejem Nowakiem – o czym świadczy archiwum GaduGadu. Z komunikacji pomiędzy obu panami wynika, iż Pan Andrzej Nowak poinstruował Pana Kowalskiego jak ukryć dane i wysłać je poprzez pocztę email.

Znalezione pliki wskazują jednoznacznie na złamanie tajemnicy przedsiębiorstwa przez Jana Kowalskiego poprzez ujawnienie danych poufnych. Dane zostały wysłane przy pomocy poczty elektronicznej po uprzednim ukryciu plików poufnych w plikach graficznych, które miały odwrócić uwagę czy uniemożliwić analizę wysłanych plików w systemie poczty elektronicznej. Pan Jan Kowalski działając z jasnym celem wysłania

⁷⁶ FCIV - File Checksum Integrity Verifier utility - <http://support.microsoft.com/kb/841290>

poufnych informacji, próbował zatrzeć ślady przechowywania plików z poufnymi danymi na swoim komputerze. Działania Pana Jana Kowalskiego były zaplanowane i przemyślane. Celem tych działań było przekazania poufnych danych firmie konkurencyjnej. Szczegółowe wnioski wraz z odtworzonym przebiegiem zdarzeń znajdują się raporcie końcowym.

⁷⁷ Raport „Forensic Investigation Report Template” - http://www.thesecurityguide.com/downloads/task,doc_details/gid,5/

PODSUMOWANIE

W pracy bazując na ogólnym modelu informatyki śledczej zaprezentowano podstawowe metody i narzędzia niezbędne do przeprowadzenia analizy dochodzeniowej w przypadku podejrzenia popełnienia przestępstwa komputerowego. Pokazano jak wykonywać dochodzenie i jak do takiego procesu się przygotować. W części praktycznej przeprowadzono badanie hipotetycznego incydentu, wykorzystując omówione wcześniej narzędzia. Efektem końcowym jest załączony do pracy raport wraz z wnioskami.

Praca ma aspekt praktyczny. W codziennej pracy administratorów systemów informatycznych, znajomość podstaw informatyki śledczej może zarówno pomóc prawidłowo przygotować i zabezpieczyć dowód elektroniczny jak i zabezpieczyć się w przyszłości przed różnego rodzaju incydentami, w tym wyciekiem informacji.

Zgłębiając tajniki informatyki śledczej musimy również pamiętać o technikach utrudniających pracę detektywów i śledczych. Są one określane terminem *anti-forensics* i mają za zadanie zabezpieczenie się przed ujawnieniem działań i zatarciem śladów popełnianych przestępstw. Do najbardziej popularnych technik należą: szyfrowanie danych, nadpisywanie skasowanych danych, czy ukrywanie danych. Jest to dziedzina dopiero się rozwijająca. W [16] przedstawiono porównanie wybranych pakietów, których zadaniem jest całkowite usunięcie plików i oznak działania w systemie. Pokazano, że nadal jeśli usuwane będą określone pliki nie jest łatwym pełne zatarcie śladów. Wszystkie z analizowanych narzędzi pozostawiały dane, które mogły mieć wartość dla analizy śledczej.

Pewnym utrudnieniem jest również to, że większość aktualnie dostępnych narzędzi informatyki śledczej wymaga wiedzy eksperckiej, chociażby w doborze odpowiednich opcji. Brakuje narzędzi w pełni zautomatyzowanych.

Niezależnie od powyższych stwierdzeń dziedzina informatyki śledczej cieszy się coraz to większą popularnością w Polsce, a jej efekty widać nawet w spektakularnych sprawach, takich jak sprawa Pani minister Jakubowskiej i skasowanego dysku oraz słynnego już słowa „lub czasopisma”.

BIBLIOGRAFIA:

1. [MWNFI] Anson Steve, Bunting Steve: *Mastering Windows Network Forensics and Investigation*, Sybex, 2007
2. [RFC3227] Brezinski D., Killalea t.: RFC 3227 - Guidelines for Evidence Collection and Archiving, February 2002 - <http://www.ietf.org/rfc/rfc3227.txt>
3. [EnCase] Bunting Steve: *EnCase Computer Forensics The Official EnCE: EnCase Certified Examiner Study Guide Second Edition*, Sybex - Willey Publishing Inc, 2008
4. Carrier Brian: *File System Forensic Analysis*, Addison Wesley Professional, 2005
5. [WFIR] Carvey Harlan: *Windows Forensics and Incident Recovery*, Addison Wesley, 2004
6. [IR CFT] Douglas Schweitzer, *Incident Response: Computer Forensics Toolkit*, Wiley Publishing, Inc., 2003
7. Mandia Kevin, Prorise Chris, Pepe Matt: *Incident Response & Computer Response, Second Edition*, McGraw-Hill/Osborne 2003
8. [MICROSOFT1] Microsoft: *Fundamental Computer Investigation Guide for Windows ver. 1.0*, January 2007,
<http://www.microsoft.com/downloads/details.aspx?FamilyId=71B986EC-B3F1-4C14-AC70-EC0EB8ED9D57&displaylang=en>
9. [FRGCF:AT] Nolan Richard, Baker Marie, Branson Jake, Hammerstein Josh, Rush Kris, Waits Cal, Schweinsberg Elizabeth: *First Responders Guide to Computer Forensics: Advanced Topics*, Carnegie Mellon University - Software Engineering Institute, September 2005,
<http://www.sei.cmu.edu/publications/documents/05.reports/05hb003/05hb003.html>
10. [WFA] Harlan Carvey: *Windows Forensic Analysis DVD Toolkit*, Syngress 2007
11. [FRGCF] Nolan Richard, O'Sullivan Colin, Branson Jake, Waits Cal : *First Responders Guide to Computer Forensics*, Carnegie Mellon University - Software Engineering Institute, March 2005-
<http://www.sei.cmu.edu/publications/documents/05.reports/05hb001.html>
12. Prorise Chris, Mandia Kevin: *Incident Response: Investigating Computer Crime*, McGraw-Hill/Osborne, 2001
13. [CF JUMPSTART] Solomon Michael G., Barrett Diane , Broom Neil: *Computer Forensics JumpStart*, Sybex 2005

14. [MICOSOFT2] - *Windows Server 2003 Resource Kit Registry Reference* -
<http://technet.microsoft.com/en-us/library/cc778196.aspx>, Microsoft Technet,
Updated: March 28, 2003
15. [NTFS TR] - *NTFS Technical Reference* -
<http://technet2.microsoft.com/windowsserver/en/library/81cc8a8a-bd32-4786-a849-03245d68d8e41033.msp?mfr=true>
16. Matthiew Geiger: *Evaluating Commercial Counter-Forensic Tools*. Digital Forensic Research Workshop, New Orleans, LA, 2005.

Prezentacje i wystąpienia na temat Informatyki śledczej autora pracy:

2008.02.20 – Prezentacja na spotkaniu merytorycznym Stowarzyszenia ISSA Polska, Warszawa –
<http://issa.org.pl>

Temat: „Computer Forensics z perspektywy administratora Windows”

Plik prezentacji: dostępny tylko dla zarejestrowanych członków Stowarzyszenia ISSA Polska

2008.09.02 – Prezentacja na spotkaniu WGSiUW - Warszawskiej Grupy Specjalistów i
Użytkowników Windows, siedziba firmy Microsoft Warszawa

Temat: „Wstęp do Computer Forensics w środowisku Windows”

Plik prezentacji:

http://ms-groups.pl/wguisw/Prezentacje/Trzecie%20spotkanie%202008.09.2008/wstep_ComputerForensics.pdf

2009.03.14 – Prezentacja na spotkaniu konferencji Communities2Communities (C2C) edycja 2009
- <http://www.communities2communities.org.pl/>

Temat: „Podążając śladami użytkownika Windows – elementy informatyki śledczej”

Plik prezentacji:

http://www.communities2communities.org.pl/Files/Materials/KB_podazajac_sladami.rar

Strony poświęcone tematyce informatyki śledczej

<http://www.iis.org.pl> – Stowarzyszenie Instytut Informatyki Śledczej

<http://www.forensicfocus.com/>

<http://www.forensicswiki.org/>

<http://www.opensourceforensics.org/>

<http://www.scm.uws.edu.au/computerforensics/>

<http://www.theseecurityguide.com/>

Załącznik 1- Wzór łańcucha dowodowego

DOWÓD ELEKTRONICZNY – ŁAŃCUCH DOWODOWY⁷⁸

Nr Przypadku:	Strona: z:
---------------	------------

OPIS SZCZEGÓŁOWY DOWODU ELEKTRONICZNEGO / KOMPUTERA

<i>Numer elementu:</i>	<i>Opis</i>		
<i>Producent:</i>	<i>Typ / model:</i>	<i>Numer seryjny:</i>	

SZCZEGÓŁY OBRAZU

<i>Data/ Czas:</i>	<i>Utworzony przez:</i>	<i>Zastosowana metoda:</i>	<i>Nazwa pliku/obrazu:</i>	<i>Segments:</i>
<i>Dysk na którym przechowano dane:</i>		<i>HASH:</i>		

ŁAŃCUCH DOWODOWY

Numer referencyjny	Data / Czas	Pobrano od:	Wydany do:	Powód
	Data:	Nazwisko/Organizacja	Nazwisko/Organizacja	
	Czas:	Podpis:	Podpis:	
	Data:	Nazwisko/Organizacja	Nazwisko/Organizacja	
	Czas:	Podpis:	Podpis:	
	Data:	Nazwisko/Organizacja	Nazwisko/Organizacja	
	Czas:	Podpis:	Podpis:	
	Data:	Nazwisko/Organizacja	Nazwisko/Organizacja	
	Czas:	Podpis:	Podpis:	

⁷⁸ Wzór dokumentu „Chain of Custody” pochodzi z pakietu Helix w wersji 1.9

Załącznik 2 – Zawartość płyt dołączonych do pracy

Płyta CD1 dołączona do pracy magisterskiej zawiera:

- Pracę magisterską w wersji elektronicznej
- Raport końcowy w wersji elektronicznej

Płyta DVD1 dołączona do pracy magisterskiej zawiera:

- kopię bitową obrazu badanego systemu
- programy i narzędzia wykorzystane do analizy
- pliki wynikowe z przeprowadzonej analizy
- plik raportu końcowego
- wykaz plików załączonych na płycie

Załącznik 3 - Raport końcowy