Helion

Informatyka śledcza

Gromadzenie, analiza i zabezpieczanie dowodów elektronicznych dla początkujących

Packt›

William Oettinger

Tytuł oryginału: Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence

Tłumaczenie: Filip Kamiński

ISBN: 978-83-283-9164-2

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/inslgr
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

2

ROZDZIAŁ

Proces analizy śledczej

Omówię teraz proces analizy śledczej. W pracy śledczego niezbędny jest proces, który umożliwi sprawne przeprowadzenie dochodzenia. Musisz się również upewnić, że znasz wykorzystywane w pracy narzędzia i rozumiesz otrzymywane z nich wyniki. Bez odpowiednio przygotowanego procesu śledczego stracisz czas na badanie danych, które nie będą miały wpływu na dochodzenie, i nie będziesz mógł polegać na swoich narzędziach. Chcesz mieć pewność, że używane przez Ciebie narzędzia dają prawidłowe wyniki. Dokładność i skuteczność wymagają krytycznego myślenia, które pomoże określić najlepszą metodę prowadzenia śledztwa lub badania.

Chociaż istnieją podobieństwa pomiędzy różnymi dochodzeniami, z czasem odkryjesz, że istnieją też różnice, które będą wymagały od Ciebie opracowania strategii gwarantującej wydajność. Nie jestem fanem tworzenia list kontrolnych określających, co należy zrobić, ponieważ istnieją obszary, które zmieniają się w zależności od śledztwa (takie jak różne systemy operacyjne, topografie sieci, rodzaje przestępstw i podejrzani). Zmienne te stanowią przyczynę, dla której żadne dwa dochodzenia nigdy nie będą takie same i będą wymagały od śledczego zastosowania innych strategii.

Proces analizy kryminalistycznej możemy podzielić na pięć etapów:

- rozważania przed dochodzeniem,
- analiza informacji o sprawie i zagadnień prawnych,
- pozyskiwanie danych,
- proces analizy,
- raportowanie wyników.

Wszystkie te etapy omówię bardziej szczegółowo w kolejnych podrozdziałach.

Rozważania przed dochodzeniem

Etap poprzedzający dochodzenie to czas na określenie możliwości i wybór sprzętu, który zostanie wykorzystany do przeprowadzenia śledztwa. Decyzje te musisz podjąć niezależnie od tego, czy praca będzie się odbywała w terenie, czy w laboratorium. Jest to moment, w którym należy ustalić budżet na sprzęt, personel i szkolenia. Niektóre z powyższych wydatków nie będą miały charakteru jednorazowego, lecz będą stanowiły część ogólnego budżetu. Sprzęt należy na bieżąco aktualizować, a personel powinien się szkolić. Wraz z pojawieniem się na rynku nowych rozwiązań koniecznie należy je zakupić.

Praca informatyka śledczego nie polega na jednorazowym zakupie sprzętu i odbyciu szkolenia. Wraz z rozwojem technologii zmieniają się również metody ukrywania danych czy prowadzenia działalności przestępczej. Śledczy musi się ciągle przystosowywać do zachodzących zmian.

Zanim rozpoczniesz śledztwo, musisz się odpowiednio przygotować. Dzięki temu zwiększysz wydajność i poprawisz efekty swojej pracy. Powinno to obejmować przygotowanie sprzętu i zapoznanie się z obowiązującymi przepisami, decyzjami prawnymi oraz politykami i procedurami przestrzeganymi w organizacji.

Niektóre urządzenia mogą być stosowane wielokrotnie, inne nie. W przypadku przedmiotów jednorazowego użytku upewnij się, że ktoś je wymieni, gdy tylko zakończy się śledztwo.

> Nie potrafię powiedzieć, ile razy stawiłem się na miejscu zdarzenia z moim „wyjazdowym" zestawem śledczym tylko po to, aby uświadomić sobie, że inny detektyw już go użył i nie wymienił jednorazowego sprzętu. Moim błędem było to, że nie sprawdziłem zestawu przed wyjazdem na miejsce zdarzenia. Błędem mojego partnera było to, że nie wymienił przedmiotów jednorazowego użytku.

Omówimy teraz sprzęt, który będziesz wykorzystywał w pracy śledczego.

Stacja robocza dla śledczego

Częstym tematem rozmów podczas spotkań z innymi śledczymi są parametry stacji roboczych wykorzystywanych w naszej pracy. W rozmowach często padają pytania takie jak: Ile pamięci RAM ma twoja stacja? Ile dysków SSD jest w tym komputerze? Jaki procesor wybrać? Z jakiego systemu operacyjnego korzystasz? Zawsze istnieją różnice zdań na temat konfiguracji stacji roboczych. Żadna z opinii nie jest błędna, ponieważ konfiguracja stacji roboczej zależy od budżetu i badanych spraw.

Stacje robocze wykorzystywane w pracy informatyków śledczych nie są tanie. W zależności od poziomu umiejętności śledczy mogą zbudować własne komputery lub kupić gotowe zestawy. Kilku sprzedawców oferuje usługę konfigurowania stacji roboczej zgodnie ze specyfikacją.

Rozważmy ofertę firmy Sumuri (*https://sumuri.com*) i jej stacje robocze Talino. Podstawowy model wyceniany jest na ok. 5000 dolarów amerykańskich i zawiera:

- procesor Intel 8700K,
- 32 GB pamięci RAM typu DDR,
- dysk SSD 512 GB.

Jest to podstawowa konfiguracja przeznaczona do prac śledczych, która nadal wymaga dodania pamięci w celu przechowywania analizowanych danych. Najmocniejsza konfiguracja kosztuje ponad 18 000 dolarów i zawiera:

- dwa 14-rdzeniowe procesory serwerowe Intel Xeon E5-2690 v4 Broadwell 2,6 GHz z 35 MB pamięci podręcznej,
- dysk SSD o pojemności 1 TB przeznaczony na system operacyjny,
- dysk SSD o pojemności 1 TB do przechowywania plików tymczasowych i przetwarzania,
- dysk SSD o pojemności 2 TB przeznaczony na bazę danych,
- kilka dysków twardych o pojemnościach od 6 do 8 TB skonfigurowanych w trybie RAID,
- 640 GB DDR4 RAM,
- kartę graficzną (GPU) z 8 GB pamięci GDDR5.

Jednym z wąskich gardeł może się okazać transfer danych. Sugeruję użycie dysków SSD, gdyż mają one znacznie większą przepustowość niż typowe dyski talerzowe. Szybki procesor i duża ilość pamięci RAM zapewniają maksymalną wydajność w przeprowadzaniu analiz kryminalistycznych. Stacje robocze nie są jednak przenośne i nie zawsze będziesz w stanie przeprowadzić analizę lub zebrać dane, pracując na komfortowej stacji roboczej. Laptopy kryminalistyczne to również drogi sprzęt. W momencie pisania tej książki laptop Talino Omega ma następującą konfigurację:

- procesor Intel Core i7 8700K,
- 64 GB pamięci RAM DDR4 2133 MHz,
- dysk SSD klasy enterprise,
- opcjonalnie dodatkowe trzy dyski SSD.

> Aby przesyłać dane przez sieć, musisz wyposażyć obie stacje robocze w gigabitowe karty sieciowe.

Jak widzisz, w informatyce śledczej nigdy za wiele procesora, pamięci RAM i miejsca na dysku. Opisany sprzęt to urządzenia z wyższej półki. Analizę kryminalistyczną możesz prowadzić również za pomocą tańszych urządzeń i nadal uzyskasz te same wyniki. Sprzęt z wyższej półki skraca czas pracy. Jeżeli pracujesz dla międzynarodowej korporacji lub dużej jednostki organów ścigania, możesz dysponować budżetem na zakup sprzętu wysokiej klasy. Mniejsze jednostki, firmy lub pracujący indywidualnie muszą ustalić budżet odpowiedni dla ich sytuacji.

Czasami istnieje konieczność opuszczenia laboratorium, co oznacza, że potrzebny będzie dodatkowy przenośny sprzęt. Omówię go poniżej.

Zestaw mobilnego reagowania

Dowody elektroniczne nie zawsze trafiają do Twojego miejsca pracy. Czasami konieczne może być zebranie dowodów w konkretnej lokalizacji. Zbieranie dowodów jest podstawowym elementem każdego badania kryminalistycznego. Tak jak w przypadku badań w laboratorium, do wykonania tego zadania potrzebne będą odpowiednie narzędzia i akcesoria. Musisz stworzyć zestaw mobilnego reagowania, który będzie zawierał odpowiednie dokumenty, długopisy oraz pojemniki do przechowywania dowodów cyfrowych.

Konfiguracja zestawu jest sprawą indywidualną. Żaden zestaw nie jest doskonały, a każdy można zawsze ulepszyć. Celem jest posiadanie wszystkiego, co niezbędne do zebrania dowodów elektronicznych. Omówię teraz niektóre elementy przydatne w mojej pracy:

- **Aparat cyfrowy** z możliwością robienia zdjęć i nagrywania wideo. Musisz udokumentować sytuację na miejscu przestępstwa w momencie przybycia. Jeśli będziesz zeznawał w sądzie, to w trakcie procesu pokażesz dokładnie, co zastałeś na miejscu przestępstwa. Niektóre służby/organizacje rejestrują również wszystkie działania prowadzone przez informatyków śledczych podczas zbierania dowodów elektronicznych.

> Jedna rada. Wyłączyłbym mikrofon, aby nie nagrywać dźwięku, ponieważ może się zdarzyć, że w trakcie pracy prowadziłeś rozmowy na temat dalszego działania, używając przy tym języka, który może być uważany za mniej profesjonalny. Rozmowy i zastosowane wyrażenia mogą być wykorzystane przez drugą stronę do odwrócenia uwagi od przedstawianych dowodów.

- **Rękawiczki lateksowe**. Rękawiczki zapewniają kilkuaspektową ochronę dowodów. Po pierwsze nie zostawiasz na dowodach odcisków palców, po drugie jesteś chroniony przed potencjalnym zagrożeniem biologicznym, które może wystąpić na miejscu zdarzenia. Mam na myśli krew, mocz, kał i każdą inną substancję biologiczną, jaka przyjdzie Ci do głowy.
- **Notatniki**. Musisz udokumentować swoje działania na miejscu przestępstwa. Notatnik to idealny sposób przechowywania tych informacji. Możesz w nim zanotować, z kim rozmawiałeś, kto zabezpieczył miejsce zdarzenia, oraz zapisać podstawowe fakty dotyczące sprawy. Wraz z rozwojem dochodzenia pojawi się wiele nowych informacji. Jeśli wszystkiego nie zapiszesz, to możesz zapomnieć, że wykonałeś jakąś czynność. W niektórych służbach i organizacjach wykonuje się też odręczne szkice obszarów, w których zabezpieczane są dowody elektroniczne. Obowiązujące Cię zasady i procedury określą, czy wymagane jest ich utworzenie.
- **Dokumentacja**. Może to być formularz zebrania materiału dowodowego, w którym dokładnie opisano, co zostało zabrane i skąd, wraz z informacjami o wszelkich znakach identyfikacyjnych lub numerach seryjnych zebranych przedmiotów.

Możesz w nim również wyszczególnić etykiety lub tagi identyfikujące przedmioty zawierające dowody elektroniczne.

- **Papierowe torebki/woreczki antystatyczne**. Pojemnik z dowodami elektronicznymi musi być umieszczony w miejscu chronionym przed nieautoryzowanym dostępem. Dowody elektroniczne są bardzo wrażliwe i chcesz mieć pewność, że nie przechowujesz ich w sposób, który może generować oddziaływania elektrostatyczne. Oddziaływania te mogą uszkodzić nośnik elektroniczny i pozbawić Cię dostępu do jakichkolwiek danych.
- **Nośniki pamięci**, czyli tradycyjne dyski talerzowe, dyski SSD i pamięci USB. Korporacyjny śledczy nie może sobie pozwolić na odłączenie serwera w celu utworzenia obrazu kryminalistycznego. W zamian wykona on kopię logów, pamięci RAM oraz katalogów użytkowników i zapisze je na nośnikach o odpowiedniej wielkości.

  Od śledczych pracujących w administracji państwowej lub organach ścigania może być wymagane wykonanie pełnej kopii kryminalistycznej danych na miejscu zdarzenia, co wiąże się z koniecznością posiadania nośników o większej pojemności. W miarę zdobywania doświadczenia będziesz w stanie dokładnie określić, jakiego sprzętu potrzebujesz do wykonywania swoich obowiązków.
- **Urządzenia blokujące zapis**. Może to być urządzenie sprzętowe, takie jak mostek Tableau TK8u USB 3.0 (*https://www.guidancesoftware.com/tableau/hardware/t8u*), który umożliwia dostęp do pamięci masowej bez zmiany jej zawartości. Gromadzenie dowodów omówię znacznie bardziej szczegółowo w rozdziale 3., „Pozyskiwanie dowodów". Alternatywą dla urządzenia fizycznego jest użycie systemu zainstalowanego na dysku rozruchowym, takiego jak Paladin Sumuri. Paladin to oparta na Ubuntu dystrybucja Linuksa, która umożliwia zbieranie dowodów elektronicznych w sposób zgodny z regułami kryminalistyki. Paladin jest dostępny za darmo na stronie firmy Sumuri pod adresem *https://sumuri.com/software/paladin*.
- **Materiał ekranujący**. Może to być folia aluminiowa, torba Faradaya lub dowolny pojemnik, który będzie blokował sygnały radiowe. Pojemnik taki przyda się podczas zabezpieczania urządzeń mobilnych. Jego użycie uniemożliwi użytkownikowi zdalne wyczyszczenie lub zresetowanie urządzenia. Należy jednak pamiętać, że po umieszczeniu urządzenia w takim pojemniku jego bateria szybko się wyczerpie, ponieważ urządzenie będzie stale próbowało połączyć się z siecią. Jeśli masz dostęp do menu urządzenia, to możesz przełączyć je w tryb samolotowy. Urządzenie nie będzie się wtedy próbowało łączyć z siecią. Upewnij się, że dokumentujesz wszelkie zmiany, jakie wprowadzasz w urządzeniu.
- **Zestaw narzędzi**. Mały zestaw precyzyjnych narzędzi z wieloma bitami służy do demontażu laptopów, komputerów stacjonarnych lub urządzeń mobilnych w celu uzyskania dostępu do nośnika danych. Upewnij się, że posiadasz różne końcówki, które pasują do śrub stosowanych przez różnych producentów. Czasami do złożenia urządzeń producenci wykorzystują dwa lub trzy rodzaje końcówek.

- **Różne drobne akcesoria**. Mogą to być dodatkowe przewody zasilające, kable do przesyłania danych, koncentratory USB, śrubki lub cokolwiek innego, co może być trudne do zdobycia w sytuacji, w której trafiasz na miejsce zdarzenia w środku nocy, a w okolicy nie ma żadnych otwartych sklepów, w których można by kupić brakujący element. Jeśli wybierasz się do obiektu komercyjnego i potrzebny Ci będzie dostęp do serwera, weź ze sobą zapasową mysz i klawiaturę. (Jeśli będziesz badał ruch w sieci, to zabierz ze sobą urządzenie typu TAP). Różne drobne akcesoria to elementy, które wydają się niepotrzebne, dopóki nie pojawisz się na miejscu i nie będziesz ich potrzebował.
- **Laptop kryminalistyczny**. Upewnij się, że zainstalowane na nim oprogramowanie jest aktualne. Warto utworzyć katalog zawierający elektroniczne wersje wszystkich formularzy i dokumentów, z których będziesz korzystał i które będziesz wypełniał, oraz wszystkie aplikacje, które mogą się przydać podczas pracy.
- **Szyfrowanie**. Jeśli zdarzenie miało miejsce za granicą, pamiętaj o zaszyfrowaniu danych, które będziesz chciał przeanalizować. Przejęcie urządzenia przez służby bezpieczeństwa lub organy celne nie jest niczym niezwykłym. Szyfrowanie danych zagwarantuje, że pozyskane informacje nie zostaną w takim przypadku ujawnione.
- **Klucze sprzętowe do oprogramowania**. Istnieją komercyjne programy, które wymagają użycia klucza sprzętowego (nośnika USB) do uruchomienia. Upewnij się, że masz ze sobą klucze, ponieważ bez nich nie będziesz mógł skorzystać z części oprogramowania.

> Oprogramowanie VirtualHere (*http://virtualhere.com/home*) umożliwia zdalne korzystanie z urządzeń USB. Do jego użycia wymagany jest dostęp do internetu w miejscu docelowym oraz w miejscu, w którym znajdują się klucze USB. Jeśli nie masz pewności co do jakości połączenia, warto zabrać klucze ze sobą.

Ważnym pytaniem jest to: *Jak przenieść wszystkie powyższe narzędzia z jednego miejsca do drugiego?*

Do ochrony sprzętu polecam walizki typu Pelican, które są wodoszczelne i odporne na uszkodzenia. Jeśli będziesz podróżował komercyjnymi liniami lotniczymi, wybierz walizkę z zamkiem TSA.

Powyższa lista to jedynie wskazówka. Sprostanie potrzebom danego zadania będzie wymagało wzbogacenia zestawu lub usunięcia niektórych jego elementów. Nie istnieją dobre lub złe zestawy mobilnego reagowania. To, jaki sprzęt zabrać, będzie zależało od zadania, budżetu i organizacji, dla której pracujesz.

W Twoim zestawie mobilnego reagowania powinny się znajdować elementy niezbędne do podjęcia działań lub zebrania dowodów w każdego rodzaju zdarzeniu. To, w co wyposażysz ten zestaw, zależy wyłącznie od Ciebie. Chodzi tylko o zwiększenie wydajności i ułatwienie Twojej pracy śledczej.

W tym punkcie omówiłem potrzeby sprzętowe i fizyczne. Przejdę teraz do omówienia oprogramowania.

Oprogramowanie śledcze

Jest to oprogramowanie, które będziesz wykorzystywał do analizy danych. Możesz wybierać pomiędzy oprogramowaniem komercyjnym i tym dostępnym na licencji *open source*. Upewnij się, że w swoim środowisku pracy korzystasz z w pełni legalnego oprogramowania. Nie ma większego wstydu niż ujawnienie w postępowaniu administracyjnym lub sądowym, że organizacja przeprowadziła dochodzenie z użyciem oprogramowania pirackiego. Korzystanie z pirackiego oprogramowania poważnie wpłynie na Twoją reputację i spowoduje pojawienie się pytań dotyczących Twojej uczciwości i zasad etycznych oraz poda w wątpliwość wyniki dochodzenia i rezultaty otrzymane w wyniku użycia nielegalnego oprogramowania. Raz jeszcze podkreślam, że w trakcie dochodzenia musisz korzystać z w pełni legalnego oprogramowania. Jaka jest więc różnica między oprogramowaniem *open source* a narzędziami komercyjnymi?

Oprogramowanie typu *open source* jest dostępne za darmo dla każdego. Zazwyczaj nie ma ograniczeń w jego stosowaniu. Możesz je wykorzystać do celów edukacyjnych, zarobkowych lub testowych. Jego zaletą jest to, że w większości przypadków jest ono bezpłatne. Do wad możemy zaliczyć niewielkie lub zerowe wsparcie techniczne w przypadku, gdy coś pójdzie nie tak. Decyzja o wyborze komercyjnego lub otwartoźródłowego oprogramowania będzie zależeć wyłącznie od Twoich umiejętności i komfortu pracy z tymi narzędziami. Zamiast **graficznego interfejsu użytkownika** (ang. *graphical user interface* — GUI) wiele narzędzi typu *open source* korzysta z **interfejsu wiersza poleceń** (ang. *command-line interface* — CLI), który nowym użytkownikom może się wydać skomplikowany.

Narzędzie komercyjne to zwykle lepsza obsługa klienta, dokumentacja i regularne aktualizacje. Minusem jest konieczność poniesienia opłaty. W rzeczywistości wszystko, co możesz wykonać, korzystając z komercyjnego narzędzia, da się zrobić również za pomocą oprogramowania typu *open source*. Program komercyjny pozwoli wykonać wiele czynności, których przeprowadzenie za pomocą darmowych odpowiedników może wymagać użycia większej liczby narzędzi.

W tym przypadku nie ma złego wyboru. Jako informatyk śledczy musisz wiedzieć, skąd pochodzą dane, i upewnić się, że narzędzie przedstawia je w dokładny sposób. Nie ma znaczenia, czy stosowany przez Ciebie program jest dostępny na licencji komercyjnej, czy *open source*. Twoim zadaniem jest walidacja wyników dostarczonych przez dowolne narzędzie. Walidację omówię w dalszej części książki.

Często otrzymuję pytania o to, czy dane oprogramowanie jest zatwierdzone do użytku w sądzie (ang. *court-approved*). Oprogramowanie kryminalistyczne nie ma takiego statusu, ale w postępowaniu administracyjnym/sądowym musisz wyjaśnić, czy narzędzie, które stosujesz, daje wiarygodne wyniki i jest akceptowane w środowisku śledczych.

W Stanach Zjednoczonych zasada ta jest znana jako standard Dauberta. Wywodzi się z rozpatrywanej przez Sąd Najwyższy sprawy Daubert przeciwko Merrell Dow Pharmaceuticals Inc. (509 U.S. 579, 1993). Standard Dauberta służy do ustalenia, czy zeznania biegłego sądowego opierają się na uzasadnionym naukowo rozumowaniu oraz czy można je zastosować do faktów w sprawie. W sprawie tej Sąd Najwyższy wziął pod uwagę następujące kwestie:

- Czy teoria lub technika może być lub została przetestowana?
- Czy poddano ją recenzji i czy została opublikowana?
- Jaki jest znany lub przewidywany poziom błędu?
- Istnienie i zachowanie standardów zastosowania.
- Akceptacja w środowisku naukowym.

Początkowo standard ten był stosowany tylko w zeznaniach o charakterze naukowym. Jednak w sprawie Kumho Tyre Co. przeciwko Carmichael (526 US 137, 1999) Sąd Najwyższy uznał, że czynniki użyte w orzeczeniu w sprawie Dauberta mogą mieć również zastosowanie do niemających charakteru naukowego zeznań inżynierów i innych ekspertów, którzy nie są naukowcami. Jak widzisz, chodzi nie tyle o oprogramowanie, ile o specjalistyczną wiedzę informatyka śledczego. Komercyjne narzędzia kryminalistyczne upraszczają proces i czasami zawierają przycisk *Znajdź dowody*. Jako informatyk śledczy nadal musisz wiedzieć, z którego miejsca w systemie plików narzędzie kryminalistyczne wyodrębniło dany artefakt.

Amerykański Narodowy Instytut Standaryzacji i Technologii (ang. *National Institute of Standards and Technology* — NIST) sponsoruje projekt CFTT (ang. *Computer Forensic Tool Testing Project*, *https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt*), który określa metodologię testowania oprogramowania wykorzystywanego w informatyce śledczej. W ramach projektu opracowano ogólną specyfikację tego typu narzędzi, procedury i kryteria testowe oraz zbiór testów i wykorzystywany w nich sprzęt. Na stronie projektu znajdziesz źródła przeznaczone do przeprowadzania testów oprogramowania śledczego. Znajdziesz tam również zbiór testowy, który pozwoli wykonać walidację oprogramowania. Dobrą praktyką jest regularne sprawdzanie wyników (co najmniej raz w roku lub za każdym razem, gdy dane narzędzie jest aktualizowane). Niezależnie od tego, czy jesteś śledczym w organach ścigania, czy w prywatnym przedsiębiorstwie, musisz mieć zaufanie do wykorzystywanych narzędzi i musisz być w stanie zeznać, że przetestowałeś i zwalidowałeś proces jego działania.

Proces walidacji oprogramowania kryminalistycznego został zakwestionowany w 2011 r. w procesie Anthony'ego Caseya. Prokuratura twierdziła, że na komputerze należącym do podejrzanego 84 razy wyszukano hasło *chloroform*. W trakcie procesu odkryto, że narzędzie wykorzystane przez informatyka śledczego błędnie zinterpretowało wartości w historii przeglądarki. Użytkownik odwiedził witrynę poświęconą chloroformowi jedynie raz, a nie, jak twierdziła prokuratura, 84 razy. Twórca oprogramowania śledczego zdał sobie sprawę z błędu w trakcie trwania procesu i powiadomił zespół procesowy o swoim odkryciu. Z tego powodu sugeruję użycie kilku narzędzi do potwierdzenia swoich podejrzeń. Możesz korzystać z dwóch rodzajów narzędzi: jednego komercyjnego i jednego darmowego lub dwóch darmowych. Musisz mieć pewność, że wykorzystywane przez Ciebie narzędzia działają, i musisz być w stanie zeznać, że je przetestowałeś i dokonałeś ich walidacji.

Przykładami narzędzi śledczych dostępnych na licencji *open source* są:

- **Autopsy**. To w pełni funkcjonalny zestaw narzędzi kryminalistycznych, które umożliwiają przeprowadzenie pełnego badania. Oprogramowanie jest dostępne za darmo i można je znaleźć na stronie *https://www.sleuthkit.org/autopsy/*.
- **SIFT Workstation**. SIFT to wirtualna maszyna, która korzysta z systemu Ubuntu z wieloma preinstalowanymi narzędziami śledczymi. Program jest bezpłatny i można go znaleźć pod adresem *https://digital-forensics.sans.org/community/downloads*.
- **Paladin Forensic Suite**. Paladin to oparta na Ubuntu bootowalna dystrybucja Linuksa, która oferuje interfejs użytkownika (*Paladin toolbox*) pozwalający skorzystać z kilku narzędzi kryminalistycznych typu *open source*. Paladin dostępny jest za darmo i można go znaleźć pod adresem *https://sumuri.com/software/paladin/*.
- **CAINE** (**Computer Aided Investigative Environment**) to darmowy projekt, który oferuje graficzny interfejs użytkownika oraz wiele narzędzi kryminalistycznych typu *open source*. Możesz go pobrać ze strony *https://www.caine-live.net/*.

To tylko kilka przykładów z listy pakietów kryminalistycznych typu *open source*. Istnieją również inne, o których nie wspomniałem. Możesz też rozważyć użycie narzędzi jednofunkcyjnych. Dopóki osiągasz cel, jakim jest znalezienie artefaktów i ujawnienie prawdy o badanej sprawie, nie ma znaczenia, z jakich narzędzi korzystasz. Kluczowe jest wykorzystanie Twojego doświadczenia i wiedzy zdobytej na szkoleniach do wyjaśnienia istotności znalezionego artefaktu i tego, w jaki sposób ustaliłeś, że użyte narzędzie daje wiarygodne wyniki.

Oto kilka komercyjnych narzędzi kryminalistycznych działających w systemie Windows:

- **X-Ways Forensics** — *https://www.x-ways.net/*.
- **EnCase** — *https://www.guidancesoftware.com/encase-forensic*.
- **Forensic Toolkit** (FTK) — *https://accessdata.com/products-services/forensic-toolkit-ftk*.
- **Forensic Explorer** (FEX) — *http://www.forensicexplorer.com/*.
- **Belkasoft Evidence Center** — *https://belkasoft.com/ec*.
- **Axiom** — *https://www.magnetforensics.com/products/magnet-axiom/*.

Dla systemu macOS dostępne są:

- **Blacklight** — *https://www.blackbagtech.com/software-products/blacklight.html*.
- **Recon Lab** — *https://sumuri.com/software/recon-lab/*.

Użytkownicy Linuksa mogą sięgnąć po narzędzie **SMART** (*http://www.asrdata.com/forensic--oprogramowanie/smart-for-linux/*).

Powyższe przykłady to jedynie wycinek z listy komercyjnych narzędzi kryminalistycznych. Każde narzędzie ma swoje mocne i słabe strony, o których można bez końca dyskutować z innymi użytkownikami.

W tej chwili moim podstawowym narzędziem jest X-Ways. Korzystam też z FEX-a i Evidence Center.

Możesz posiadać odpowiednie narzędzia, sprzęt i oprogramowanie, ale czy bez właściwego przeszkolenia będziesz skuteczny? W kolejnym punkcie omówię kilka możliwości szkolenia.

Szkolenia dla śledczych

Jeśli zdecydujesz się na karierę w informatyce śledczej, to będziesz musiał nieustannie doskonalić swoje umiejętności. Uczestnictwo w szkoleniach należy traktować jako stały wydatek. To, że jakaś osoba odbyła 40-godzinny kurs, wcale nie oznacza, że automatycznie jest ona informatykiem śledczym. Wprawdzie to pierwszy krok na drodze do tego zawodu, ale taka osoba nadal powinna brać udział w sesjach szkoleniowych i spotykać się z innymi zainteresowanymi tą tematyką.

Certyfikat nie gwarantuje, że jego posiadacz wie, co robi, a jedynie pokazuje, że osiągnął on minimalny poziom wiedzy wymagany do jego zdobycia. Istnieje *wiele* certyfikatów, a niektóre z nich są bardziej wartościowe niż inne. Przed dołączeniem do organizacji i rozpoczęciem certyfikacji starannie zbadaj koszty, dostępność oraz to, czy dany certyfikat jest akceptowany w środowisku informatyków śledczych. Większość organizacji certyfikujących będzie wymagała opłacania składek i corocznego szkolenia w celu odnowienia ważności certyfikatu.

Poniżej wymieniłem kilka organizacji oferujących szkolenia z zakresu kryminalistyki:

- **International Association of Computer Investigative Specialists (IACIS)** — *https://www.iacis.com/*.
- **EnCase Certified Examiner (EnCE)** — *https://www.opentext.com/products-and-solutions/services/training-and-learning-services/encase-training/examiner-certification*.
- **Accessdata Certified Examiner (ACE)** — *https://accessdata.com/training/computer-forensics-certification*.
- **Computer Hacking Forensic Investigator (CHFI)** — *https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/*.
- **Global Information Assurance Certification (GIAC)** — *https://www.giac.org/certifications*.

Po omówieniu sprzętu i możliwości szkoleniowych przejdę do kwestii prawnych i szczegółów sprawy związanych ze specyfiką dochodzenia. Zacznę od kwestii prawnych.

Analiza informacji o sprawie i zagadnień prawnych

Porozmawiajmy o informacjach o sprawie i kwestiach prawnych. Są to informacje, które musisz uzyskać, zanim włączysz swoją stację roboczą, aby przejrzeć dowody elektroniczne. Część z tych informacji będziesz musiał pozyskać od osoby korzystającej z Twoich usług. Powinieneś jej zadać następujące pytania:

- Jaki jest charakter dochodzenia? Czy jest to sprawa narkotykowa, zabójstwo czy wykroczenie pracownika? W trakcie słuchania formułuj plan dalszego działania.
- Jakie dowody elektroniczne spodziewasz się zastać na miejscu zdarzenia? Kiedyś otrzymałem odpowiedź, że powinienem szukać tylko jednego laptopa, a po przybyciu na miejsce wraz ze współpracownikami znaleźliśmy wiele laptopów, wiele komputerów stacjonarnych i wiele urządzeń mobilnych. Pamiętaj, że informacje, które otrzymujesz, mogą nie być dokładne. Musisz być przygotowany na taką ewentualność.
- Jaka jest podstawa prawna? W przypadku organów ściągania: jakie są przesłanki do przeszukania? Zgoda? Nakaz? Nie ma znaczenia, czy jest to pisemna zgoda, czy nakaz przeszukania. Musisz zapoznać się z tymi dokumentami, aby się upewnić, że rozumiesz ograniczenia związane z zezwoleniem. Mogą to być ograniczenia fizyczne zezwalające na przeszukanie jedynie miejsca przestępstwa lub ograniczenia cyfrowe dotyczące tego, czego możesz szukać na urządzeniach cyfrowych.
- W mojej karierze rządowego i korporacyjnego informatyka śledczego często występowały ograniczenia w zakresie tego, co mogłem przeglądać i wyszukiwać na urządzeniach cyfrowych. Bądź świadomy tych ograniczeń. Jeśli znajdziesz artefakty poza dozwolonym obszarem, to nie będą one mogły być użyte w postępowaniu, a z ich wykorzystaniem mogą się wiązać sankcje.
- Kim są ofiary i podejrzani oraz jaką rolę odgrywają w śledztwie? W zależności od Twojej roli możesz mieć (lub nie) kontakt z ofiarami i podejrzanymi. Jeśli masz taką możliwość, spróbuj z nimi porozmawiać. Jeśli Ci się uda, być może zyskasz dodatkowe informacje o nośnikach i ich zawartości.

Mylisz się, jeśli sądzisz, że po zebraniu informacji od uczestników zdarzenia i funkcjonariuszy, którzy jako pierwsi pojawili się na miejscu zdarzenia, możesz od razu zabrać się za gromadzenie dowodów. Najpierw musisz się upewnić, że miejsce przestępstwa zostało odpowiednio udokumentowane. W przypadku organów ścigania proces ten obejmuje usunięcie osób postronnych, ograniczenie dostępu i zarejestrowanie stanu w miejscu zdarzenia.

Najłatwiej jest wszystko sfotografować. Być może będziesz składał swoje zeznania dopiero za 12, 18, 24 lub nawet więcej miesięcy. W trakcie procesu prawnicy mogą zapytać Cię, gdzie znajdował się określony przedmiot. Jeśli nie będziesz dysponował zdjęciem (lub szkicem) miejsca zdarzenia, to być może nie zdołasz odpowiedzieć na to pytanie.

Co zrobić w przypadku śledztwa korporacyjnego? Na przykład gdy znaleziono ukrytą kamerę? Działania znalazcy mogą utrudnić Twoją pracę. Prowadziłem kiedyś sprawę, w której we wspólnej toalecie znaleziono ukrytą kamerę. Korzystający z toalety zobaczył kamerę na podłodze po tym, jak zerwała się taśma, za pomocą której kamera była przymocowana do spodu półki. Następnie osoba ta oddała kamerę swojemu przełożonemu. Przełożony rozmontował kamerę i wyjął z niej kartę pamięci, którą umieścił w czytniku kart, a ten następnie podłączył do swojego komputera. Zanim się ze mną skontaktowano, kamera i karta SD były w rękach co najmniej pięciu osób, a karta została podłączona do kilku komputerów. Każde podłączenie karty SD do komputera powoduje zmianę dowodów. Dostęp do danych znajdujących się na karcie powoduje zmiany w znacznikach czasowych plików. Firma powinna przeszkolić swoich pracowników i poinformować ich, że w przypadku incydentu należy wezwać specjalistę i powstrzymać się od przeglądania dowodów elektronicznych. Takie działanie zagwarantuje, że dowody będą się znajdowały w stanie umożliwiającym ich przedstawienie w sądzie lub postępowaniu administracyjnym.

Ten przypadek wymagał przesłuchania wszystkich zaangażowanych osób, zbadania aparatu cyfrowego i karty SD oraz pięciu stacji roboczych. Ponieważ rzecz działa się w środowisku korporacyjnym, początkowo nie planowano angażowania organów ścigania. W celu późniejszej identyfikacji konkretnych urządzeń i ich użytkowników sfotografowałem stacje robocze i podłączone do nich przewody. Pamiętaj, że działałem w środowisku korporacyjnym, w którym prawie każdy komputer to ten sam model tego samego producenta.

Czasami będziesz analizował dowody elektroniczne zebrane przez kogoś innego. W takich przypadkach nadal musisz zadawać pytania, ale źródłem odpowiedzi będą jedynie raporty śledcze. Będziesz chciał ustalić następujące kwestie:

- Dlaczego przedmiot został zabezpieczony?
- Czy przedmiot zawiera dowody działalności przestępczej lub dowody uniewinniające?
- Czy istnieje łańcuch dowodowy związany z tym przedmiotem?
- Ile osób miało dostęp do tego przedmiotu?
- Gdzie znaleziono ten przedmiot?
- Czy przedmiot został znaleziony w miejscu z ograniczonym dostępem, czy na terenie ogólnodostępnym?
- Kiedy znaleziono przedmiot (data i czas)?
- Na czym powinno się skoncentrować dochodzenie?
- Do kiedy należy przedstawić wyniki analizy?

Przed rozpoczęciem procesu zbierania dowodów musisz zapoznać się z dokumentacją sprawy. Gdy otrzymasz dowody, takie jak komputery, upewnij się, że nakaz przeszukania umożliwił ich zajęcie. Zdarzały się przypadki zajęcia urządzeń zawierających dowody elektroniczne, w których analiza zawartości stanowiła działanie w szarej strefie.

Nakaz przeszukania będzie zawierał ograniczenia dotyczące Twojej działalności. Jeśli będzie to dochodzenie dotyczące nielegalnych zdjęć, Twoje działania mogą być ograniczone jedynie

do przeglądania tego rodzaju treści. Twoim obowiązkiem jest zapoznanie się ze wszystkimi dokumentami sądowymi i zrozumienie, do czego Cię one upoważniają, a do czego nie. Tylko wtedy będziesz mógł opracować plan, który pozwoli Ci działać w granicach prawa.

Musisz również przewidzieć problemy, jakie mógłbyś napotkać podczas przeprowadzania cyfrowego badania kryminalistycznego. Czy jest jakiś aspekt dochodzenia, w którym problemem mogą być braki w Twoich umiejętnościach lub doświadczeniu? Nie są to kwestie, których należy się wstydzić, ale powinieneś być ich świadomy, aby wiedzieć, kiedy sięgnąć po środki, które rozwiną Twoje umiejętności i doświadczenie. Z jakich zasobów możesz skorzystać?

Po omówieniu kwestii prawnych związanych z przygotowaniem procesu analizy przejdę do opisania tego, jak należy pozyskiwać dane zgodnie ze sztuką kryminalistyczną.

Pozyskiwanie danych

Ustalmy więc, że przeszedłeś szkolenie z zakresu informatyki śledczej i być może uzyskałeś jakiś certyfikat. Zbudowałeś lub kupiłeś stację roboczą oraz laptopa z przeznaczeniem do prowadzenia śledztw oraz skompletowałeś zestaw mobilnego reagowania. Dotarłeś na miejsce przestępstwa i upewniłeś się, że zostało ono zabezpieczone. Ustaliłeś też, że nikt nie naruszył miejsca przestępstwa, i wykonałeś jego dokumentację fotograficzną. Nadszedł czas, abyś wkroczył na miejsce i zebrał dowody. Omówię teraz pozyskiwanie danych, innymi słowy: zbieranie dowodów.

Istnieje wiele sytuacji, w których możesz zostać poproszony o zebranie dowodów elektronicznych na potrzeby śledztwa. Jako funkcjonariusz organów ścigania możesz wkroczyć na miejsce przestępstwa, zidentyfikować potencjalne źródła dowodów elektronicznych, a następnie zająć te przedmioty. W sektorze prywatnym lub korporacyjnym możesz zostać poproszony o zajęcie stanowiska pracy pracownika lub przeprowadzenie czynności w serwerowni (zdalnie lub na miejscu) w celu zebrania danych, które chcesz przeanalizować. Procedury, które omówię poniżej, można zastosować w każdym środowisku.

Źródłem potencjalnych dowodów jest pamięć ulotna. W przeszłości zgodnie z regułą „wyciągnij wtyczkę" zawarte w niej dane były ignorowane. Reguła ta dotyczyła sytuacji, w których funkcjonariusze znajdowali na miejscu przestępstwa uruchomiony komputer. Zgodnie z obowiązującymi w tamtym czasie praktykami funkcjonariusze byli zobowiązani do „wyciągnięcia wtyczki" w celu wyłączenia urządzenia. Pamięć ulotna jest dostępna tylko wtedy, gdy komputer jest uruchomiony. Po wyjęciu wtyczki funkcjonariusze kopiowali wszystkie potencjalne dowody. W miarę rozwoju informatyki śledczej nauczyliśmy się, że to, co kiedyś uważaliśmy za najlepszą praktykę, w rzeczywistości nie było dobre.

W trakcie zbierania ulotnych dowodów powinniśmy zacząć od tych, które najłatwiej utracić. Kolejność zbierania dowodów jest następująca (tzw. *order of volatility*):

1. Działające systemy komputerowe.
2. Aplikacje działające w systemie.

3. Sieć.
4. Dowody wirtualne.
5. Dowody fizyczne.

Do gromadzenia ulotnych danych powinieneś podejść w taki sam sposób, jak do wykonywania obrazów kryminalistycznych. Musisz udokumentować wykonywane kroki, ponieważ w celu zebrania ulotnych danych będziesz wchodził w interakcję z maszyną. Interakcja ta zmieni dowody. W rzeczywistości zmiany, które wprowadzisz, zazwyczaj nie wpływają na to, co badasz. Powinieneś jednak wiedzieć, że w systemie dokonywane są zmiany. Podczas składania zeznań ktoś może Cię zapytać o ewentualne zmiany w materiale dowodowym. Profesjonalista powinien umieć odpowiedzieć na takie pytanie.

Zmiany wprowadzone podczas zapisywania ulotnych danych wpłyną na zawartość pamięci RAM. Dlatego musisz robić notatki i dokumentować wszystko, co czynisz. Przykładami ulotnych danych są informacje o: sieci (tabela ARP, istniejące połączenia, tabela routingu i pamięć podręczna), tym, kto jest aktualnie zalogowany, działających w systemie usługach i procesach, współdzielonych dyskach, aktywności zdalnej i aktualnie otwartych zaszyfrowanych kontenerach.

Musisz znaleźć równowagę pomiędzy wprowadzanymi przez Ciebie zmianami a dowodami, które mogą zostać na zawsze utracone. Określenie „zgodnie z regułami kryminalistyki" oznacza pozostawienie jak najmniejszego śladu podczas zbierania dowodów, tak aby zminimalizować ilość modyfikowanych danych. Kolejność gromadzenia nietrwałych danych jest istotna. Jeśli zgromadzisz ulotne dane w złej kolejności, możesz zniszczyć dowody, których szukasz. Pamięć RAM jest uważana za najbardziej ulotną ze wszystkich rodzajów pamięci. To od niej powinieneś rozpocząć zbieranie danych.

Pamiętaj o następujących kwestiach:

- Zależnie od okoliczności przestępstwa zebranie ulotnych danych może nie być zawsze możliwe.
- Jeśli ustalisz, że na komputerze działa proces, który modyfikuje lub nadpisuje interesujące Cię dane, możesz uznać, że nie warto poświęcać czasu na zapis pamięci RAM, ponieważ przechowywane w niej dowody mogły zostać zmanipulowane.
- Jeśli źródłem tego procesu jest czynnik zewnętrzny (połączenie zdalne), musisz udokumentować, a następnie zerwać połączenie oraz zapisać zawartość pamięci RAM. Szczegóły będą zależne od rodzaju dochodzenia i informacji, które próbujesz zdobyć.
- Jeśli atakujący jest podłączony zdalnie i ma dostęp do wrażliwych danych, to czy chcesz, aby osoba ta zachowała dostęp podczas gromadzenia pamięci RAM, czy wolisz zerwać połączenie? Co zrobić, jeśli nie są to informacje krytyczne?
- Czy chcesz, by atakujący miał dostęp do systemu w trakcie zbierania dowodów?

Ostatecznie celem informatyka śledczego jest przygotowanie obrazu kryminalistycznego do analizy. W standardowych okolicznościach nie powinno się modyfikować dowodów elektronicznych podczas ich gromadzenia.

W dzisiejszych czasach nie zawsze jest to możliwe. Ze względu na popularność szyfrowania dysku lub pełnego szyfrowania woluminów strategia „wyciągania wtyczki" nie jest już dopuszczalna.

Zmieńmy na chwilę temat i porozmawiajmy o tym, czym jest szyfrowanie. Na podstawowym poziomie szyfrowanie polega na kodowaniu informacji w celu ochrony ich poufności. Szyfrowanie umożliwia dostęp do danych jedynie osobie posiadającej klucz deszyfrujący. Szyfr może zostać złamany, jeśli atakujący ma wystarczająco dużo czasu.

Przy obecnym sprzęcie czas potrzebny na złamanie szyfrowania mierzy się w setkach lat, ale wraz z postępem technologicznym i ze wzrostem mocy komputerów czas niezbędny do złamania najbardziej złożonych szyfrów skraca się. To, co w latach 90. uważano za bezpieczny algorytm szyfrujący, dziś jest już traktowane jako słabe zabezpieczenie. Właśnie z tego powodu nie należy odłączać od zasilania systemów, w których możliwe jest użycie szyfrowania. Bez dostępu do klucza deszyfrującego nie będziesz w stanie dostać się do danych.

Każda sytuacja, każde miejsce zdarzenia i każde śledztwo są inne. Oznacza to, że podejmowane przez Ciebie działania będą zależeć od okoliczności. Wykorzystaj swoją umiejętność rozwiązywania problemów i podejmuj szybkie decyzje na podstawie dostępnych informacji.

Masz już dowody — w jaki sposób powinieneś przejąć nad nimi kontrolę? Porozmawiamy teraz o łańcuchu dowodowym.

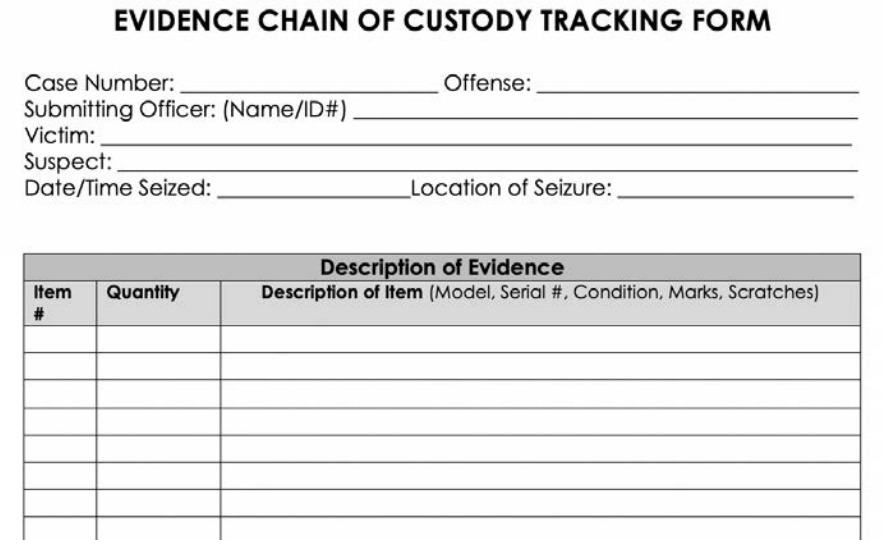
Łańcuch dowodowy

Łańcuch dowodowy (ang. *chain of custody*) stanowi integralną część procesu zabezpieczenia i uwierzytelnienia fizycznych i elektronicznych dowodów w postępowaniu administracyjnym lub sądowym. Łańcuch ten dokumentuje proces dostępu do materiału dowodowego i określa, kto miał do niego dostęp, kiedy i w jakim celu.

Na stronach NIST znajdziesz dokument łańcucha dowodowego pokazany na rysunku 2.1. Jest to wzór ogólnego przeznaczenia, który możesz dostosować do swoich potrzeb. Znajdziesz go pod adresem *https://www.nist.gov/document/sample-chain-custody-formdocx*. Formularz jest przeznaczony do prowadzenia łańcucha dowodowego i powinien być uzupełniany za każdym razem, gdy dowód zostanie przekazany z rąk do rąk.

Jak widzisz, niektóre pola mogą nie być Ci potrzebne. Na przykład jeśli jesteś korporacyjnym informatykiem śledczym, to pewnie nie przyda Ci się pole *Victim* (ofiara). Możesz je zmienić lub całkowicie je usunąć.

Celem tego formularza jest śledzenie pracy z dowodem elektronicznym i zachowanie nad nim kontroli, tak aby móc później uwierzytelnić dowody. W polu *Description of Evidence* (opis dowodu) należy opisać nośnik zawierający dowód. Może to być np. nośnik jednorazowego użytku, taki jak płyta DVD, na której nagrano logi przeznaczone do dalszej analizy.



EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Rysunek 2.1. Formularz dowodowy

Na rysunku 2.2 pokazano sekcję *Description of Evidence*. Kolumna *Item* (przedmiot) zawiera identyfikator, który pomaga zapanować nad dowodami. W kolumnie *Quantity* (ilość) umieszcza się liczbę elementów, które opisano w kolumnie *Description of Item* (opis przedmiotu).

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
CD-001	1	Ultimate DVD contains servers log from AD001
HD-001	1	Samsung SSD 1TB Ser#ABC9876
HD-002	1	Samsung SSD 512 MB Ser# DEF4567
CP-001	1	Pixel XL 128 MB Ser# A5 12 D3 AC FD
TD-001	1	Generic Thumb drive 32MB (green) unknown SN
MD-001	1	Apple iPad 512mb Ser# 09 E3 4D AB Rose Gold

Rysunek 2.2. Opis dowodów

Na przykład na powyższej liście płyta DVD jest opisana jako pozycja *CD-001*. Możesz mieć problem z rozróżnieniem płyt, jeśli zabezpieczysz kilka płyt CD lub DVD. Problem ten nie dotyczy jedynie płyt CD/DVD, ale też dysków twardych. Konfiskaty pojedynczych nośników określonego rodzaju zdarzają się rzadko.

W mojej pracy korzystam z następującego schematu numeracji:

- Płyty CD/DVD — *CD-XXX*.
- Dyski twarde — *HD-XXX*.

- Pamięci przenośne — *TD-XXX*.
- Telefony komórkowe — *CP-XXX*.
- Inne urządzenia mobilne — *MD-XXX*.

> Musisz trwale oznaczyć zabezpieczane przedmioty. Powinieneś starać się to zrobić w sposób, który nie zmniejszy ich wartości.

Na rysunku 2.3 możesz zobaczyć, że dysk twardy został oznaczony symbolem *HDD001* oraz datą i inicjałami funkcjonariusza, który zabezpieczył to urządzenie.

Rysunek 2.3. Dysk twardy

Po utworzeniu obrazu kryminalistycznego urządzenie będzie przez resztę procesu określane jako *HDD001*.

Jeśli nie możesz oznaczyć urządzenia bez trwałego zmniejszenia jego wartości (np. jest to iPad), nie korzystaj z trwałego markera. W zamian użyj etykiety samoprzylepnej.

> Wybierz system, który będzie się sprawdzał w Twoim przypadku. Po opracowaniu sposobu numeracji upewnij się, że korzystasz z niego za każdym razem. Uchroni Cię to przed utratą dowodów lub ich błędnym oznaczeniem.

Podczas zabezpieczania dowodów i nośników cyfrowych na miejscu przestępstwa powinieneś mieć pewność, że czynności te są przeprowadzane zgodnie z regułami kryminalistyki. Nie analizuje się oryginalnych dowodów, lecz utworzone w tym celu kopie. Takie działanie pozwala zagwarantować, że nie wprowadzisz żadnych zmian w oryginalnych dowodach.

Istnieją trzy możliwości wykonania kopii roboczej:

- **Kopia kryminalistyczna** (ang. *forensic copy*). Są to po prostu dane z nośnika dowodowego skopiowane bit po bicie. Ten rodzaj kopii nie jest obecnie popularny. Jeśli wykonujesz taką kopię, upewnij się, że urządzenie docelowe nie zawiera danych z wcześniejszych analiz. Nie możesz doprowadzić do sytuacji, w której zmieszaniu ulegną dane z obecnego i poprzedniego dochodzenia. Ten rodzaj kopii pozwala odzyskać usunięte pliki oraz zawartość niewykorzystanych przestrzeni na końcach plików i partycji. Proces wymazywania dysków twardych omówię w dalszej części tej książki.
- **Obraz kryminalistyczny** (ang. *forensic image*). Jest to stworzona bit po bicie kopia urządzenia źródłowego, którą zapisano w formacie przeznaczonym do analizy kryminalistycznej, np. jako obraz DD, E01 lub AFF. W tym rodzaju kopii oryginalne dane są umieszczone w chroniącym je kontenerze, którym jest format kryminalistyczny. Ten rodzaj kopii pozwala odzyskać usunięte pliki oraz zawartość niewykorzystanych przestrzeni na końcach plików i partycji.
- **Logiczny obraz kryminalistyczny** (ang. *logical forensic image*). Czasami możemy uzyskać dostęp jedynie do określonego zbioru danych i nie mamy możliwości (lub zgody) na dostęp do całego kontenera. W takich przypadkach nie możemy stworzyć bitowego obrazu kryminalistycznego lub kopii kryminalistycznej. Sytuacja taka może wystąpić np., gdy wyodrębniamy dane z serwera, którego nie możemy wyłączyć w celu utworzenia obrazu kryminalistycznego jego dysków twardych. W ten sposób możemy tworzyć logiczne kopie plików i folderów związanych z dochodzeniem. W tym przypadku nie będziemy w stanie odzyskać usuniętych plików oraz zawartości niewykorzystanych przestrzeni na końcach plików i partycji.

W rozdziale 3., „Pozyskiwanie dowodów", zajmiemy się tworzeniem obrazu kryminalistycznego z urządzeń lub danych zabezpieczonych na miejscu zdarzenia.

Teraz, gdy omówiłem już, co należy wziąć pod uwagę przy pozyskiwaniu danych, przejdę do procesu ich analizy.

Proces analizy

Po zabezpieczeniu danych na miejscu przestępstwa i powrocie do laboratorium nadszedł czas, aby rozpocząć analizę kryminalistyczną. Dość szybko poczujesz się przytłoczony ilością danych, które znajdziesz na urządzeniach pamięci masowej. Musisz szybko ustalić, czy informacje zapisane na tych nośnikach mają znaczenie dla Twojego śledztwa. Na tym etapie kluczową rolę odegrają wyniki z etapu gromadzenia informacji o sprawie i analizy kwestii prawnych.

Musisz wziąć pod uwagę, kto, co, kiedy, gdzie, dlaczego i jak (wspominałem o tym w rozdziale 1., „Rodzaje dochodzeń w informatyce śledczej"). Powiąż aktywność w systemie komputerowym z konkretną osobą i spróbuj określić, kto to taki.

Jeśli w dochodzeniu zidentyfikowano już podejrzanego, powiąż go z użytkownikiem w systemie komputerowym. Niektóre omówione poniżej działania możesz przeprowadzić za pomocą dowolnego komercyjnego lub darmowego oprogramowania kryminalistycznego. Moim celem jest przedstawienie procesu bez uciekania się do konkretnego narzędzia.

Daty i strefy czasowe

Jeżeli się o nich zapomni, kwestie związane z datą i ze strefami czasowymi mogą powodować problemy w pracy informatyków śledczych. Jeśli prowadzisz analizę w określonej strefie czasowej i wszystkie przechwycone dane również z niej pochodzą, to nie będziesz miał w zasadzie żadnych problemów. Jeśli jednak dane pochodzą z wielu stref czasowych lub podróżujesz pomiędzy obszarami leżącymi w różnych strefach czasowych, kwestie te mogą wprowadzić pewne zamieszanie, jeśli nie weźmiesz ich pod uwagę.

Rozwiązaniem jest ustawienie na komputerze i w oprogramowaniu strefy **czasu uniwersalnego** (UTC). Upewnij się również, że dostosowałeś do niego wszystkie znaczniki czasowe związane z działalnością przestępcy. Pewnym utrudnieniem jest to, że systemy operacyjne zapisują metadane w wielu różnych strefach czasowych. Musisz również wziąć pod uwagę, że podejrzany mógł zmienić ustawienia strefy czasowej, aby ukryć swoją działalność. Analiza osi czasu ma kluczowe znaczenie podczas przeprowadzania badania kryminalistycznego.

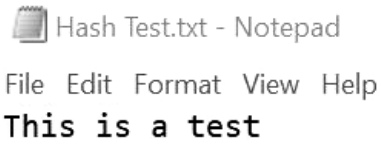
W dalszej kolejności będziesz musiał zidentyfikować nieistotne pliki, a także nielegalne zdjęcia/obrazy. Możesz to zrobić za pomocą analizy skrótów.

Analiza skrótów

Co to jest wartość skrótu/hash? Hash to „cyfrowy odcisk palca" pliku lub fragmentu treści multimedialnych. Jest on generowany przy użyciu jednokierunkowego algorytmu kryptograficznego.

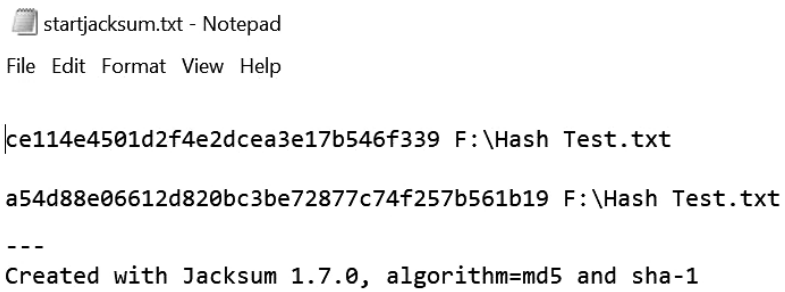
Standardowe algorytmy kryptograficzne stosowane w kryminalistyce cyfrowej to **Message Digest 5** (MD5) i **Secure Hashing Algorithm** (SHA-1). Algorytm MD5 zwraca 128-bitowy cyfrowy skrót, a SHA-1 160-bitowy. Algorytm haszujący pozwala przetworzyć dane wejściowe o zmiennej długości w wyjściowe o stałej liczbie bitów. Zmiana chociażby jednego bitu w danych wejściowych spowoduje zwrócenie innego skrótu. Przyjrzyjmy się działaniu hashy w następujących krokach:

1. Utwórz plik tekstowy *Hash Test.txt* zawierający tekst *This is a test* (rysunek 2.4).



Rysunek 2.4. Tekst, którego skrót będziemy chcieli obliczyć

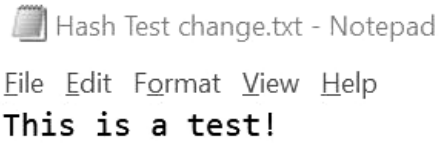
2. Oblicz wartość skrótu/hash za pomocą darmowego narzędzia Jacksum (*https://jacksum.loefflmann.net/en/index.html*) — rysunek 2.5.



Rysunek 2.5. Wartości zwrócone przez Jacksum

Jak możesz zobaczyć na rysunku 2.5, `ce114e4501d2f4e2dcea3e17b546f339` to skrót pliku *F:\Hash Test.txt* obliczony za pomocą algorytmu MD5 (ma on standardową długość). Skrótem obliczonym za pomocą algorytmu SHA-1 jest `a54d88e06612d820bc3be72877c74f257b561b19`. Rodzaj użytego oprogramowania nie ma znaczenia. Powyższe wartości to unikatowe odciski palca dla tego pliku.

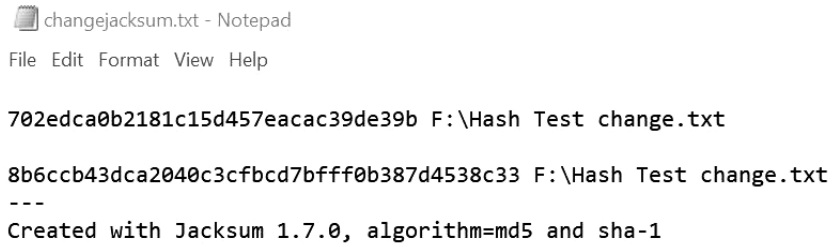
3. Zmień fragment zawartości pliku (rysunek 2.6).



Rysunek 2.6. Zmiana w tekście

Na rysunku 2.6 dodałem wykrzyknik na końcu zdania. Choć bardzo niewielka, każda zmiana spowoduje zmianę wartości skrótu.

4. Ponownie zastosuj Jacksum, aby się przekonać, że otrzymasz inne wartości (rysunek 2.7).



Rysunek 2.7. Zmiana wartości zwracanych przez Jacksum

Hash MD5 to teraz `702edca0b2181c15d457eacac39de39b`. Jest to inna wartość niż otrzymane poprzednio `ce114e4501d2f4e2dcea3e17b546f339`.

Obliczanie skrótu jest procesem jednokierunkowym. Nie da się wprowadzić wartości alfanumerycznej, aby odwrócić proces i odzyskać dane przekazane do algorytmu. Jeśli dysponujesz zbiorem hashy znanych Ci nielegalnych zdjęć, to na ich podstawie nie możesz odtworzyć ich zawartości.

Istnieją zbiory skrótów identyfikujących znane pliki, które nie interesują śledczych. Mogą to być np. pliki używane w systemie operacyjnym lub przez jakieś aplikacje. Użycie takiego zestawu skrótów pozwala odfiltrować pliki, które nie mają wartości dowodowej. Z drugiej strony znajomość hashy plików takich jak nielegalne zdjęcia lub skradzione dokumenty również może się przydać. W przypadku znanych plików związanych z działalnością przestępczą skrót może obliczyć jedynie ktoś, kto ma do nich dostęp.

Wykorzystanie analizy skrótów w toku dochodzenia może zaoszczędzić Ci trochę czasu i wysiłków:

- Możesz ją wykorzystać do sprawdzenia, czy dowody się nie zmieniły.
- Możesz posłużyć się nią do wykluczania pewnych plików.
- Możesz ją zastosować do identyfikacji interesujących Cię plików.

NIST stworzył projekt **NSRL** (ang. *National Software Reference Library*, *https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl*), w którym zebrano oprogramowanie z wielu źródeł i utworzono referencyjny zbiór danych **RDS** (ang. *Reference Data Set*). RDS to duży zbiór skrótów, który pomaga zidentyfikować znane, „dobre" pliki podczas przeprowadzania badania. Baza RDS jest dostępna dla organów ścigania, agencji rządowych i sektora prywatnego. Niektóre pliki opisane w RDS, takie jak oprogramowanie do hakowania, mogą zostać uznane za podejrzane. Śledczy musi umieścić badane pliki w kontekście, aby sprawdzić, czy nie były one wykorzystywane do celów niezgodnych z prawem. RDS nie zawiera skrótów nielegalnych danych, takich jak zakazane zdjęcia/obrazy.

Kolizja to zjawisko, w którym dwie różne zmienne wejściowe dają w wyniku tę samą wartość o stałej długości. Oznacza to, że dwa różne pliki mają tę samą wartość skrótu, co jak sobie zdajesz sprawę (na podstawie tego, co napisałem wcześniej), nie jest pożądane podczas identyfikacji dowodów. Służby państwowe podjęły działania mające na celu uzyskanie takich samych hashy dla różnych danych wejściowych. Prace te zakończyły się sukcesem.

Czy fakt ten oznacza, że haszowanie jest bezużyteczne? Otóż nie. Nie znaleziono jeszcze dwóch różnych, zwyczajnych plików, które mają taką samą wartość skrótu. Wszystkie kolizje, które udało się znaleźć, były efektem użycia plików, które zostały zmanipulowane. Pliki te nie zawierały żadnej treści czytelnej dla użytkownika. Chociaż istniały obawy, że odkrycie to wpłynie negatywnie na dopuszczalność dowodów elektronicznych, w sprawie Stany Zjednoczone przeciwko Schmidtowi sąd orzekł, że prawdopodobieństwo kolizji plików jest niewielkie i nie stanowi dla sądu problemu.

Teraz, gdy ustaliliśmy, czym jest cyfrowy odcisk palca, czas się upewnić, że pliki zostały prawidłowo zidentyfikowane.

Analiza sygnatur plików

Kolejnym krokiem jest przeprowadzenie analizy sygnatury pliku, czyli upewnienie się, że zawartość odpowiada typowi pliku. Wiele formatów plików, które występują w systemach plików, zostało ustandaryzowanych i ma unikalne sygnatury, za pomocą których odbywa się ich identyfikacja w systemie plików. Sygnatury te to nie rozszerzenia, takie jak np. *.doc* lub *.docx* znane z programu Microsoft Word.

Użytkownik może zmienić rozszerzenie pliku, aby ukryć obciążające go dowody. Celem analizy sygnatur jest ustalenie, czy sygnatura i rozszerzenie pliku są zgodne.

Na rysunku 2.8 pokazano, jak oprogramowanie X-Ways oznacza plik, w którym rozszerzenie nie jest zgodne z sygnaturą.

Name	10534.gif
Type	jpg
Description	existing
Existent	✓
Size	3.0 KB (3,081)
Modified	07/12/2008 21:51:38 +0
Ext.	gif
Type status	mismatch detected, OK
Type descr.	JPEG

Rysunek 2.8. Niezgodność w sygnaturze pliku

Rozszerzenie pliku wskazuje na format GIF, ale oprogramowanie X-Ways zidentyfikowało dane jako obrazek w formacie JPEG. Na rysunku 2.9 pokazano nagłówek pliku, który jest rzekomo w formacie GIF.

```
Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15      ANSI ASCII
00000000  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 00 00 01  ÿØÿà  JFIF
```

Rysunek 2.9. Nagłówek pliku

Sygnatura pliku GIF powinna się zaczynać od szesnastkowych liczb `47 49 46 38`, a nie `FF D8 FF E0`. W niektórych przypadkach niezgodność wynika z działania systemu plików, a nie z czynności wykonywanych przez użytkownika. Musisz zbadać dane, aby upewnić się, że powstanie niezgodności można przypisać konkretnemu użytkownikowi.

Gary Kessler stworzył stronę internetową, która umożliwia przeszukiwanie bazy danych na podstawie rozszerzenia pliku lub sygnatury pliku (rysunek 2.10). Znajdziesz ją pod adresem *https://filesignatures.net/*.

Rysunek 2.10. filesignatures.net

Bazę możesz przeszukiwać według rozszerzenia lub sygnatury pliku. Po wpisaniu rozszerzenia, którym jest w tym przypadku JPG, otrzymasz sygnatury plików związane z formatem JPEG (rysunek 2.11).

Rysunek 2.11. Wyniki dla sygnatury pliku JPG

Po upewnieniu się, że pliki zostały poprawnie zidentyfikowane, musisz zidentyfikować wszelkie złośliwe oprogramowanie, które może znajdować się w systemie. Możesz to zrobić za pomocą programu antywirusowego.

Antywirus

Prawie w każdym prowadzonym przeze mnie dochodzeniu spotkałem się z próbą obrony polegającą na twierdzeniu: „To dzieło wirusa komputerowego". Jak ustalić, czy jest to zasadne roszczenie? Czy w systemie zostało zainstalowane złośliwe oprogramowanie i czy spowodowało ono badane przez Ciebie zachowanie bez interakcji lub wiedzy użytkownika?

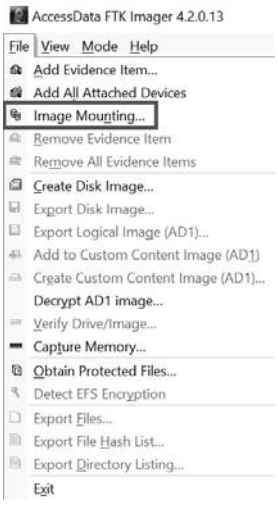
Możliwość zbadania tego, co działo się w systemie w momencie gromadzenia dowodów, jest jednym z powodów, dla których zapisujemy dane ulotne. Jeśli dowody zebrał ktoś inny, a Ty dysponujesz jedynie obrazem kryminalistycznym, to nadal możesz go przeskanować, by ustalić, czy w systemie zostało zainstalowane złośliwe oprogramowanie. Część oprogramowania kryminalistycznego pozwala na „zamontowanie" obrazu w trybie tylko do odczytu i przeskanowanie systemu plików w celu ustalenia, czy zainstalowano złośliwe oprogramowanie.

Przykładem oprogramowania, które pozwala zamontować obraz kryminalistyczny, jest bezpłatne narzędzie FTK Imager oferowane przez firmę AccessData. Znajdziesz je pod adresem *https://accessdata.com/product-download/ftk-imager-version-4.2.0*.

Możesz zamontować obraz kryminalistyczny lub nośnik fizyczny. Dane będziesz przeglądał w trybie tylko do odczytu. Montaż obrazu kryminalistycznego ma wiele korzyści, w tym możliwość przeglądania obrazu za pomocą Eksploratora plików na zasadach takich, jakby było to urządzenie podłączone do komputera. Dzięki temu możesz przeglądać różne typy plików za pomocą natywnych narzędzi, skanować obraz za pomocą antywirusa, udostępniać zamontowany obraz w sieci i kopiować z niego pliki.

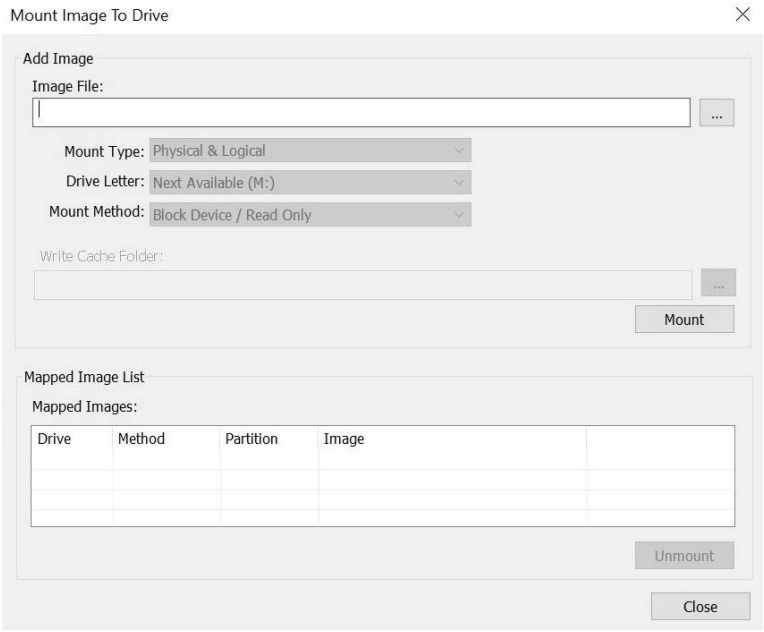
Omówię teraz, jak zamontować obraz kryminalistyczny za pomocą narzędzia FTK Imager:

1. Aby zamontować obraz kryminalistyczny, wybierz opcję *Image Mounting…* (montowanie obrazu) z menu *File* (plik), tak jak pokazano na rysunku 2.12.



Rysunek 2.12. Montowanie obrazu

2. Na ekranie (rysunek 2.13) wyświetli się menu *Mount Image to Drive* (zamontuj obraz jako dysk).



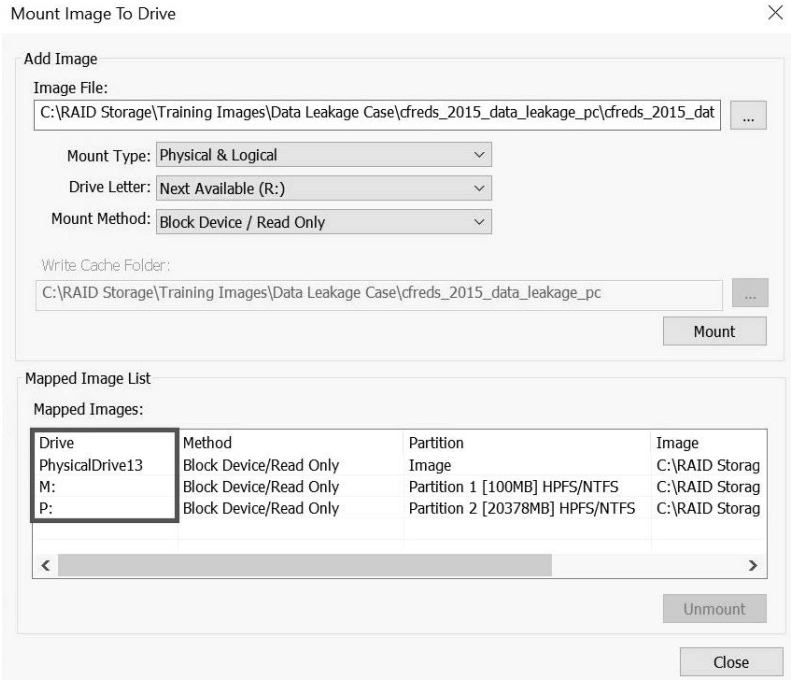
Rysunek 2.13. Montowanie obrazu

W oknie dialogowym musisz wybrać obraz kryminalistyczny, który chcesz zamontować. Jeśli jest to obraz podzielony na segmenty, wystarczy wskazać jego pierwszy element:

- *Mount Type* (rodzaj montowania). Masz do wyboru tryby: *Physical&Logical* (fizyczny i logiczny), *Physical* (tylko fizyczny) lub *Logical* (tylko logiczny). W przypadku wybrania pierwszej opcji oprogramowanie zamontuje obraz jako urządzenie fizyczne, a także zamontuje wszystkie jego partycje logiczne.
- *Drive Letter* (litera dysku). Określa literę, pod którą zostanie zamontowany obraz. Na rysunku 2.13 widać, że następną dostępną wolną literą jest *M*. Możesz też wybrać każdą inną wolną literę.
- *Mount Method* (metoda montażu). Istnieją następujące możliwości montażu:
  - *Block Device/Read Only* (urządzenie blokowe/tylko do odczytu). Opcja ta spowoduje potraktowanie urządzenia jako blokowego, co oznacza, że zamontowane urządzenie będzie mogła wyświetlić aplikacja w systemie Windows, która wykonuje zapytania o fizyczne nazwy urządzeń.
  - *Block Device/Writable* (urządzenie blokowe/zapisywalny). W tym trybie wszystkie zmiany są zapisywane w pamięci podręcznej. Tryb ten nie narusza oryginalnych dowodów.

- *File System/Read-Only* (system plików/tylko do odczytu). Urządzenie jest montowane w trybie tylko do odczytu. Możliwe jest przeglądanie zawartości za pomocą Eksploratora plików w systemie Windows.

Na rysunku 2.14 pokazano zrzut ekranu, na którym zamontowałem obraz kryminalistyczny zawierający kilka partycji.



Rysunek 2.14. Zamontowany obraz

Zamontowałem partycje jako dyski *M* i *P*. Po zamontowaniu możesz przeskanować zamontowane partycje za pomocą programu antywirusowego, aby sprawdzić, czy znajduje się na nich złośliwe oprogramowanie.

Sama obecność złośliwego oprogramowania nie stanowi alibi dla podejrzanego. Musisz sprawdzić, czy znalezione oprogramowanie może wykonać czynności, które zarzuca mu podejrzany. W swojej pracy prowadziłem wiele spraw z tytułu posiadania nielegalnych treści, w których oskarżony twierdził, że materiały te zostały pobrane przez złośliwe oprogramowanie. Nie znam żadnego oprogramowania, które wyszukuje, znajduje, pobiera i sortuje nielegalne materiały znalezione na komputerze podejrzanego. Pamiętaj, że aby określić kontekst, nadal musisz przeanalizować zawartość.

Teraz możesz zająć się analizą systemu plików i systemu operacyjnego. Konkretne artefakty omówię w dalszej części tej książki. Dla jasności: **system operacyjny** (OS od ang. *operating system*) to system służący do komunikacji między aplikacjami a warstwą sprzętową.

Najpopularniejsze systemy operacyjne to Microsoft Windows, macOS i Linux. Prawie każda czynność wykonywana w systemie operacyjnym, niezależnie od tego, czy została wykonana przez człowieka, czy maszynę, pozostawi ślad gdzieś w systemie operacyjnym. Dlatego aby ustalić, czy użytkownik zrobił coś niewłaściwego, warto przeanalizować artefakty w systemie operacyjnym.

System plików to mechanizm przechowywania danych. System ten jest niezależny od systemu operacyjnego. System plików śledzi liczbę dostępnego miejsca w pamięci oraz to, gdzie przechowywane są dane. Istnieje wiele systemów plików, np.: NTFS, HFS+, FAT 32 i Ext 4. Niektóre z nich są kompatybilne z wieloma systemami operacyjnymi, inne nie. Na przykład system NTFS jest stosowany w systemie operacyjnym Microsoft Windows.

Gdy masz pewność, że w systemie nie ma złośliwego oprogramowania, możesz przejść do raportowania wyników.

Raportowanie wyników

Doszliśmy do ostatniego etapu pracy, czyli raportowania. Na tym etapie wykonałeś już całą pracę związaną z przygotowaniem, zakupem sprzętu, odbyciem szkoleń i skompletowaniem zestawu mobilnego reagowania, a gdy nadeszło wezwanie, udałeś się na miejsce zdarzenia. Zebrałeś z sukcesem informacje o sprawie i orientujesz się w kwestiach natury prawnej. Zapisałeś ulotne dane, zidentyfikowałeś nośniki zawierające cyfrowe dowody i zabezpieczyłeś je zgodnie z zasadami kryminalistyki. Zadbałeś też o łańcuch dowodowy podczas transportu dowodów do laboratorium. Następnie przeprowadziłeś analizę i znalazłeś artefakty, które dowodzą, że podejrzany wykonał lub nie zarzucane mu czyny.

Co teraz? Musisz być w stanie wyjaśnić swoje ustalenia osobie nietechnicznej. W tym celu musisz przedstawić bardzo techniczne zagadnienia w sposób zrozumiały dla osoby nietechnicznej. Jest to jeden z najtrudniejszych aspektów bycia informatykiem śledczym. Konieczne może być stworzenie różnych wersji raportu skierowanych do różnych odbiorców. Adresaci Twojego raportu przeczytają go i odpowiednio zinterpretują, a Ty możesz zostać poproszony o złożenie zeznań przed sądem lub w postępowaniu administracyjnym.

Szczegóły do uwzględnienia w raporcie

W raporcie musisz podać wystarczająco dużo szczegółów, tak abyś był w stanie przypomnieć sobie, co się wydarzyło. Pomocne może być robienie notatek na wszystkich etapach sprawy. Sam wiele razy nie skorzystałem z tej możliwości i z tego powodu musiałem powtórzyć pewne czynności, ponieważ nic nie zapisałem. Twoje notatki mogą mieć różne formy, takie jak odręczne zapiski, tekst napisany na maszynie lub komputerze, zrzuty ekranu oraz notatki sporządzone za pomocą funkcjonalności dostępnych w Twoim ulubionym oprogramowaniu kryminalistycznym. Poza tym, że należy je prowadzić, nie istnieją dobre ani złe reguły dotyczące robienia notatek.

A więc co chcesz udokumentować? Oto kilka kwestii, które warto rozważyć:

- Komunikacja między głównym śledczym a prokuratorem.
- Stan pojemników dowodowych.
- Specyfika nośników pamięci (marka, model, numer seryjny i stan).
- Dane osobowe podejrzanych, ofiar i świadków.
- Zastosowany w śledztwie sprzęt.
- Użyte oprogramowanie.
- Rzeczy, które zbadałeś (nawet jeśli badanie nie wykazało niczego, co miałoby wartość dowodową).
- Twoje ustalenia.

Zbierz razem wszystkie te elementy i połącz je w taki sposób, aby nietechniczny odbiorca zrozumiał, co się działo w śledztwie, jakie kroki podjąłeś i dlaczego wyciągnąłeś takie wnioski. Podobnie jak w innych dziedzinach, w informatyce śledczej nie ma ustalonego formatu raportu. Musisz opierać się na wymaganiach pracodawcy, odbiorców raportu i swoich preferencjach.

Polecam uwzględnić w raporcie następujące informacje. Warto podzielić go na trzy główne części:

- opis działań,
- analiza znalezionych dowodów,
- dodatkowa dokumentacja.

Opis działań nie wymaga większych wyjaśnień. Musisz opisać, co się wydarzyło, co zrobiłeś i jakie to ma znaczenie. Powinieneś zacząć od krótkiego streszczenia, w którym wymienisz kluczowe aspekty i wnioski, a następnie przejść do szczegółowego opisu. W opisie powinieneś umieścić zrzuty ekranu odnoszące się do omawianych artefaktów. Nie zamieszczaj zrzutów niezwiązanych z opisem. Nie zakładaj, że czytelnik zrozumie, co przedstawia zrzut. Musisz to wyjaśnić. Upewnij się, że zrzut ekranu skupia się na omawianym artefakcie.

Jeśli Twój raport zawiera zrzuty ekranu przedstawiające rzeczy zabronione, takie jak nielegalne obrazy, musisz zachować kontrolę, aby nie doszło do przypadkowego ujawnienia tych materiałów. Będziesz też musiał sporządzić drugi raport, pozbawiony tych materiałów, przeznaczony dla czytelników, którzy nie mają prawa wglądu w takie treści.

Po streszczeniu należy umieścić podstawowe informacje o charakterze administracyjnym. Wymień osoby zaangażowane w sprawę, w tym ofiary, podejrzanego, świadka i innych śledczych.

Udokumentuj fakty i okoliczności

W dalszej części raportu powinieneś opisać fakty i okoliczności śledztwa. Kiedy wszczęto dochodzenie? Jakie działania podjęli inni śledczy przed rozpoczęciem Twoich prac? Powinieneś uwzględnić też podstawę przeszukania.

Przeanalizowane dowody możesz wymienić na dwa sposoby. W niektórych większych sprawach wykaz dowodów elektronicznych może zająć dwie lub więcej stron. Długa lista dowodów nie ułatwi czytelnikowi zrozumienia raportu. Bardziej prawdopodobne jest, że czytelnik pominie listę dowodów i przejdzie dalej. Jeśli dochodzenie nie obejmowało badania dużej liczby urządzeń cyfrowych, możesz je wymienić. Na takiej liście należy umieścić też urządzenia, w których nie znalazłeś niczego, co miało wartość dla sprawy. Jeśli liczba urządzeń jest długa, sugeruję wymienić tylko te, które zawierały artefakty mające znaczenie w sprawie, a całą listę dowodów zamieścić na końcu raportu.

W raporcie powinieneś również podać szczegóły dotyczące tworzenia obrazów kryminalistycznych. Zazwyczaj umieszczam podsumowanie tego procesu w części opisującej moje działania. Następnie w części dowodowej umieszczam szczegółowy opis prezentujący krok po kroku proces uzyskania obrazu kryminalistycznego. Szczegółowy opis tego procesu umieszczony w części opisowej nie pomoże czytelnikowi w zrozumieniu całego procesu. Przekazanie mu podstawowych informacji o procesie tworzenia obrazu i uszczegółowienie ich w innej części zwiększa czytelność raportu.

Analiza dowodów cyfrowych będzie stanowiła większość Twojego raportu. W tej części przeprowadzasz czytelnika krok po kroku przez proces odkrywania artefaktów i ich znaczenia dla sprawy. Wiele razy widziałem raporty, w których dany obraz kryminalistyczny był określany jako ważny bez wyjaśnień „dlaczego". Czy znaczenie ma miejsce, w którym znaleziono obraz, czy istotna jest jego zawartość? Staraj się wyjaśnić, dlaczego konkretny artefakt jest ważny i na jakiej podstawie to stwierdziłeś.

> Pamiętaj, że przedstawiasz techniczne zagadnienia nietechnicznym odbiorcom. Nie możesz stworzyć listy ważnych plików i założyć, że czytelnik będzie wiedział, co jest ważne.

Uważam, że najlepiej jest prezentować artefakty w porządku chronologicznym. Na przykład jeśli badasz sprawę nielegalnego pobierania materiałów chronionych prawem autorskim, możesz zacząć od ustalenia, kto jest potencjalnym właścicielem komputera i wszelkich artefaktów, które mogą pozwolić zidentyfikować konkretnego użytkownika. Następnie możesz zaprezentować wszystkie wyszukiwania, które użytkownik przeprowadził w celu znalezienia chronionych materiałów, oraz opisać kroki podjęte w celu ich pobrania. Jeśli użytkownik komunikował się z innymi, a tematem tych rozmów były materiały chronione prawem autorskim, to możesz zastosować te wiadomości do poparcia swojej hipotezy dotyczącej tego, że oskarżony dopuścił się pobrania materiałów chronionych prawem autorskim.

Możesz również zaprezentować artefakty według tematów. Jeśli badasz posiadanie i rozpowszechnianie nielegalnych obrazów, możesz najpierw przedstawić artefakty wskazujące, że użytkownik oglądał te materiały. To pokaże, że użytkownik wiedział o istnieniu tych plików w swoim systemie, a także, czy aktywnie udostępniał je innym. Sam obraz nie wystarczy. Musisz również znaleźć artefakty wspierające Twoje hipotezy dotyczące udostępniania obrazów. W trakcie pisania części dotyczącej analizy należy unikać jakichkolwiek bezwzględnych stwierdzeń. Widziałem raporty dotyczące posiadania nielegalnych obrazów, gdzie śledczy bezwzględnie twierdził, że użytkownik wiedział o nielegalnych zdjęciach, które zostały

znalezione w pamięci podręcznej nośnika USB. Obecność materiału w pamięci podręcznej nie jest bezwzględnym dowodem na to, że użytkownik wiedział o fotografii. Dane mogą być umieszczane w pamięci podręcznej nośnika bez wiedzy użytkownika. Musisz uważać, jaki język stosujesz. Nie zamieszczaj opinii. Przedstaw tylko informacje.

Widziałem raporty opisujące artefakt jako „nieprzyzwoite zdjęcie dziecka". Termin „nieprzyzwoite zdjęcie" nie jest oparty na faktach. Jest to opinia. Opis artefaktu powinien być rzeczowy i pozbawiony Twoich odczuć. Lepszym opisem tej fotografii mogłoby być „zdjęcie przedstawiające nagiego młodo wyglądającego mężczyznę znajdującego się w zalesionej okolicy". Uważaj, jak opisujesz artefakty przypisane do konkretnego użytkownika lub osoby. Najtrudniej jest udowodnić, kto siedział za klawiaturą. Jeżeli nie dysponujesz nagraniem z przestępstwa, to nigdy nie możesz powiedzieć, że podejrzany A ze stuprocentową pewnością popełnił zarzucany mu czyn. Ta część raportu to nie miejsce, w którym możesz wyrazić swoją opinię. Nie zakładaj, że wiesz na pewno, kto jest właścicielem przedmiotu ani jaka jest tożsamość użytkownika.

Podsumowanie raportu

Ostatnią częścią szczegółowego opisu jest wniosek. To część, w której możesz wyrazić własną opinię na podstawie artefaktów opisanych w sekcji analizy. Nadal musisz uważać na swoje opinie. Spróbuj spojrzeć na artefakty bez z góry przyjętych założeń i ustal, czy fakty potwierdzają Twoją hipotezę. Jeśli nie potrafisz zdecydować, zapisz tę informację. Pamiętaj, że nie zawsze chodzi o udowodnienie winy. Możesz również musieć przedstawić dowody na to, że podmiot nie popełnił zarzucanych mu czynów.

Prawdopodobnie będziesz musiał stworzyć elektroniczną wersję raportu. W jej przypadku najczęściej używanym formatem jest PDF. Bez względu na to, jaki format wybierzesz, upewnij się, że raport został opatrzony podpisem elektronicznym. Potwierdzi on, że treść raportu nie uległa zmianie od czasu jego podpisania.

> Pamiętaj, że raport reprezentuje Twoją osobę i dochodzenie. Jeśli napiszesz kiepski raport, odbije się on negatywnie na Tobie, śledztwie i Twojej organizacji.

Korekta raportu jest niezbędna. Nie sprawdzaj go samodzielnie, bo przeoczysz różne kwestie, takie jak błędy typograficzne, niezrozumiałe zdania i niejasne ustalenia. To, co może Ci się wydawać jasne, nie zawsze jest zrozumiałe po zapisaniu. Jeśli śledztwo przekształci się w postępowanie administracyjne lub sądowe, gwarantuję, że obrońcy przeanalizują Twój raport zdanie po zdaniu, szukając niespójności i miejsc, w których nie byłeś obiektywny.

Pamiętaj, że jeśli czytelnik nie rozumie tego, co napisałeś o znalezionych artefaktach, oznacza to, że cały Twój wysiłek pójdzie na marne.

Podsumowanie

W tym rozdziale omówiłem proces analizy kryminalistycznej. Wiesz już, jak przygotować się do przeprowadzenia analizy materiałów elektronicznych. Wiesz, jakiego sprzętu będziesz potrzebował, jakie szkolenia powinieneś odbyć i jakie certyfikaty powinny być warte Twojej uwagi. Rozumiesz, jak ważne jest zebranie informacji przed zabezpieczeniem dowodów i upewnienie się, że porozmawiałeś z innymi śledczymi lub personelem zaangażowanym w zdarzenie.

Nie znajduję sposobu na wystarczające podkreślenie znaczenia ulotnych danych. Jeśli ich nie zabezpieczysz, stracisz dużą liczbę potencjalnych dowodów. W tym rozdziale opisałem kilka strategii przeprowadzania analizy oraz różnice między artefaktami z systemu operacyjnego oraz artefaktami z systemu plików. Na koniec omówiłem raportowanie wyników w sposób zrozumiały dla osób czytających Twój raport.

W następnym rozdziale zajmiemy się szczegółami gromadzenia dowodów oraz sposobem walidacji narzędzi wykorzystywanych do tworzenia pozbawionego błędów obrazu kryminalistycznego.

Pytania

1. Które z poniższych elementów powinny się znaleźć w Twoim zestawie mobilnego reagowania?
   a. Kamera cyfrowa.
   b. Rękawiczki lateksowe.
   c. Urządzenie blokujące zapis.
   d. Wszystkie powyższe odpowiedzi.
2. Do przeprowadzenia poprawnej analizy kryminalistycznej niezbędne jest płatne oprogramowanie.
   a. Prawda.
   b. Fałsz.
3. Jakie pytania należy zadać po otrzymaniu dowodów cyfrowych?
   a. Dlaczego zabezpieczono ten dowód?
   b. Gdzie jest łańcuch dowodowy?
   c. Kto miał dostęp do dowodów?
   d. Wszystkie powyższe.
4. Pamięć RAM jest najbardziej ulotnym dowodem.
   a. Prawda.
   b. Fałsz.
5. Łańcuch dowodowy opisuje _____.
   a. kto miał dostęp do dowodów,

b. kto był świadkiem,

c. odciski palców podejrzanego,

d. żadna z powyższych.

6. Który z niżej wymienionych rodzajów kopii sprawdzi się najlepiej podczas badania dowodów elektronicznych?

a. Kopia kryminalistyczna.

b. Obraz kryminalistyczny.

c. Logiczny obraz kryminalistyczny.

d. Odpowiedzi b i c.

7. Który z poniższych algorytmów jest algorytmem haszującym?

a. CDC.

b. FBI.

c. MD5.

d. LSD.

Poprawne odpowiedzi znajdziesz na końcu książki.

Materiały dodatkowe

W. Kruse i J. Heiser, *Computer Forensics: Incident Response Essentials*, Addison Wesley, 2001.

Jak prowadzić cyberśledztwo. Zabezpieczanie i analiza dowodów elektronicznych

Przestępcy sięgają po coraz to nowsze metody. Inżynierowie potrafią wykrywać ślady nielegalnych działań, jeśli jednak celem jest ujęcie i ukaranie sprawcy, potrzeba czegoś więcej. Zadaniem śledczego jest nie tylko przeprowadzenie badań, ale również zabezpieczenie i analiza dowodów, wreszcie — przedstawienie wyników swojej pracy tak, aby można ich było użyć w postępowaniu sądowym. By tak działać, konieczne jest przyswojenie zasad informatyki śledczej.

Ta praktyczna książka zawiera omówienie reguł, jakimi powinien się kierować informatyk śledczy podczas pracy. Przedstawia podstawy kryminalistyki, stanowi też przegląd narzędzi i technik służących do skutecznego badania cyberprzestępstw, a także do efektywnego zbierania, utrwalania i wykorzystywania dowodów elektronicznych. Duży nacisk położono tu na techniki pozyskiwania danych z systemu Windows: opisano sposoby zbierania artefaktów w różnych wersjach systemu, zaprezentowano sposoby analizy pamięci RAM i poczty e-mail w kontekście prowadzenia dochodzenia. Ważną częścią publikacji są rozdziały dotyczące pisania raportów i zasad, których musi przestrzegać biegły sądowy w ramach swojej pracy.

Dzięki książce dowiesz się:

- czym jest proces dochodzeniowy i jakie są zasady pracy z dowodami
- jakie narzędzia kryminalistyczne pozwalają na efektywną pracę
- na czym polega proces rozruchu z użyciem BIOS-u, UEFI i sekwencji rozruchowej
- jak pozyskiwać wartościowe dane znajdujące się w sieci i na urządzeniach
- jak lokalizować i wykorzystywać najpopularniejsze artefakty systemu Windows
- z czym się wiąże udział w postępowaniu sądowym lub administracyjnym

William Oettinger jest emerytowanym oficerem policji w Las Vegas i emerytowanym agentem kryminalnym Korpusu Piechoty Morskiej Stanów Zjednoczonych. Ma ponad dwudziestoletnie doświadczenie w pracy w organach ścigania. Specjalizuje się w informatyce śledczej, egzekwowaniu prawa, dochodzeniach karnych, a także we wdrażaniu polityk i procedur cyberbezpieczeństwa.

Dowiedz się, jak powstrzymać cyberprzestępcę!

Packt

Helion

helion.pl

HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-283-9164-2

Cena: 79,00 zł