WYDANIE II

INFORMATYKA W KRYMINALISTYCE

PRAKTYCZNY PRZEWODNIK

DR DARREN R. HAYES

Tytuł oryginału: A Practical Guide to Digital Forensics Investigations (2nd Edition)

Tłumaczenie: Tomasz Walczak

ISBN: 978-83-283-7569-7

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/inwkr2
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

Rozdział 1

Zakres informatyki śledczej

Efekty nauki

Po lekturze tego rozdziału będziesz rozumieć następujące zagadnienia:

- Definicja i znaczenie informatyki śledczej
- Różne rodzaje dowodów elektronicznych i sposoby ich wykorzystywania
- Umiejętności, szkolenia i edukacja niezbędne, by zostać informatykiem śledczym
- Perspektywy zatrudnienia w obszarze informatyki śledczej
- Historia informatyki śledczej
- Amerykańskie i międzynarodowe organy prowadzące dochodzenia z wykorzystaniem informatyki śledczej

Informatyka śledcza (ang. *digital forensics*) zajmuje się zbieraniem, analizą i wykorzystywaniem dowodów elektronicznych w postępowaniach cywilnych i karnych. Ciekawe jest to, że w informatyce śledczej (nazywanej też kryminalistyką cyfrową) źródłem dowodów są nie tylko komputery. Dla informatyków śledczych potencjalnym źródłem dowodów jest dowolny nośnik, na którym przechowywane mogą być pliki cyfrowe. Informatyka śledcza obejmuje więc analizę plików cyfrowych.

Informatyka śledcza jest nauką, ponieważ istnieją przyjęte praktyki zbierania i analizowania dowodów oraz zasady ich dopuszczalności w sądzie. Ponadto narzędzia używane do zbierania i analizowania dowodów elektronicznych przez lata przechodzą wiele testów naukowych. Angielskie słowo *forensics* oznacza między innymi „odpowiedni dla sądu". Z tego wynika, że dowody elektroniczne używane w postępowaniu muszą być zbierane, przechowywane i analizowane w sposób *zgodny z obowiązującymi zasadami postępowania*. Oznacza to, że w trakcie zbierania dowodów elektronicznych i w procesie śledczym dowody muszą zachować pierwotny stan. Ponadto każda osoba mająca kontakt z dowodami musi zostać uwzględniona i zaprotokołowana w **łańcuchu dowodowym**.

Informatyka śledcza skutkuje czasem uzyskaniem **dowodów obciążających** w sprawach karnych. Jednak dowody mogą też być używane jako **dowody uniewinniające**, które świadczą o niewinności oskarżonego.

Popularne mity z dziedziny informatyki śledczej

Wiele osób uważa, że bezpieczeństwo teleinformatyczne i informatyka śledcza to jedno i to samo. Są to jednak różne dziedziny. Jest to jedno z kilku błędnych założeń z obszaru informatyki śledczej. Bezpieczeństwo teleinformatyczne jest proaktywne i służy ochronie systemów komputerowych i poufnych danych (w tym własności intelektualnej). Informatyka śledcza jest reaktywna i z natury ma charakter śledczy. Oznacza to, że przestępstwo mogło już zostać popełnione. Obie te dziedziny często łączą się w ramach reagowania na incydenty. Niektóre poważne incydenty, na przykład włamania do sieci, wymagają wiedzy informatyków śledczych, którzy próbują ustalić, co się stało i jaki jest zakres szkód, a także kto może być sprawcą. Umiejętności i techniki z obszaru informatyki śledczej często są potrzebne do zbierania informacji, nie zawsze w celu oskarżenia kogokolwiek (na przykład do analizy urządzeń mobilnych w celu sprawdzenia, czy państwo używa aplikacji do profilowania użytkowników). Ponadto techniki informatyki śledczej nieraz służą do monitorowania i zbierania informacji na temat wykorzystywania mediów społecznościowych przez znane lub potencjalne organizacje terrorystyczne. W następnych punktach opisałem wybrane błędne przekonania na temat informatyki śledczej.

Mit nr 1. Informatyka śledcza i bezpieczeństwo teleinformatyczne to jedno i to samo

Bezpieczeństwo teleinformatyczne jest proaktywne i służy między innymi ochronie komputerów i danych przed kradzieżą lub niewłaściwym wykorzystaniem. Informatyka śledcza ma działać reaktywnie i polega na szukaniu dowodów elektronicznych po popełnieniu przestępstwa w celu wyjaśnienia okoliczności oraz zidentyfikowania i skazania przestępcy. Informatyka śledcza może być uzupełnieniem bezpieczeństwa teleinformatycznego (zwłaszcza w obszarze reagowania na incydenty). Zauważ jednak, że amerykańska Narodowa Akademia Nauk uznaje informatykę śledczą za poddziedzinę cyberbezpieczeństwa.

Mit nr 2. Informatyka śledcza polega na analizowaniu komputerów

Z dalszych rozdziałów książki dowiesz się, że informatycy śledczy mogą badać dowolne urządzenia przechowujące pliki. Na przykład karta SIM telefonu komórkowego nie jest komputerem, natomiast może zawierać ważne dowody elektroniczne.

Mit nr 3. Informatyka śledcza dotyczy dochodzeń w sprawie przestępstw informatycznych

Często mylnie się uważa, że informatyka śledcza dotyczy tylko przestępstw związanych z komputerami lub cyberprzestępstw. Informatyka śledcza jest jednak równie ważna w dochodzeniach dotyczących morderstw, oszustw czy szpiegostwa przemysłowego. Na przykład 16 kwietnia 2007 roku Seung-Hui Cho zamordował 32 osoby i zranił wiele innych w kampusie Virginia Tech, po czym popełnił samobójstwo. Informatycy śledczy zbadali komputer Cho, aby wyjaśnić okoliczności. Doprowadziło to do śledztwa. Zbadano konto pocztowe Cho, Blazers5505@hotmail.com, i aktywność tego człowieka (nazwa użytkownika blazers5505) w serwisie eBay. Informatycy śledczy zdołali ustalić, z kim Cho się komunikował i czego szukał oraz co kupił w internecie. Zbadano też telefon komórkowy sprawcy. Jednym z powodów błyskawicznej reakcji informatyków śledczych była konieczność szybkiego ustalenia, czy Cho nie miał wspólnika.

Gdy agenci federalni pod koniec 2001 roku przeszukiwali biura Enronu, ustalili, że pracownicy niszczyli duże ilości dokumentów. Informatycy śledczy byli potrzebni do uzyskania dowodów z dysków twardych komputera. Szacuje się, że ilość odzyskanych danych elektronicznych była mniej więcej dziesięciokrotnie większa od zawartości Biblioteki Kongresu.

Mit nr 4. Informatyka śledcza służy do odzyskiwania usuniętych plików

Głównym zadaniem informatyki śledczej jest zbieranie i analizowanie plików za pomocą sprzętu i oprogramowania z wykorzystaniem metod naukowych dopuszczanych przez sąd. Możliwości informatyki śledczej znacznie wykraczają poza odzyskiwanie usuniętych plików. Narzędzia z obszaru informatyki śledczej pozwalają uzyskać wiele plików, do których dostęp jest utrudniony. Ponadto takie narzędzia są bardzo przydatne do wyszukiwania i filtrowania informacji. Wiele profesjonalnych narzędzi umożliwia też łamanie haseł i szyfrów. Te funkcje udostępniają na przykład narzędzia FTK i Password Recovery Toolkit (PRTK) firmy AccessData.

Zadanie praktyczne

Zasada wymiany Locarda

Doktor Edmond Locard (1877 – 1966), kryminolog z Uniwersytetu w Lyonie, opracował teorię nazywaną *zasadą wymiany*. Zgodnie z nią, gdy przestępca wchodzi w interakcje ze środowiskiem, następuje wymiana dowodów:

> Gdziekolwiek stanie, czegokolwiek dotknie, cokolwiek pozostawi — nawet nieświadomie — może posłużyć za niemego świadka przeciwko niemu. Chodzi tu nie tylko o odciski palców lub ślady stóp, ale też o włosy, włókna z odzieży, rozbitą szklankę, ślady narzędzi, zarysowaną farbę czy krew albo nasienie, które pozostawił lub które pozostały na nim. Wszystkie te i inne dowody niemo świadczą przeciwko niemu. Takie dowody nie zapominają. Nie mylą się z powodu chwilowych emocji. Nie są nieobecne, co zdarza się ludziom. Są to faktyczne dowody. Fizyczne dowody nie mogą się mylić, nie popełniają krzywoprzysięstwa i nie są nieobecne. Jedyne, co może zmniejszyć ich wartość, to niepowodzenia ludzi w ich znajdowaniu, analizowaniu i rozumieniu.

Ta teoria dotyczy też informatyki śledczej, gdzie śledczy musi znać całe środowisko, z jakim przestępca wchodził w kontakt. Dlatego ważne jest, aby śledczy nie ograniczał się do znalezionego w mieszkaniu laptopa, ale pomyślał też o tym, co jest z owym urządzeniem związane — o połączeniach z routerem, zewnętrznych dyskach twardych czy danych w chmurze. Także pamięć USB i płyty CD w mieszkaniu mogą zawierać ważne dowody. Loginy i hasła mogą być zapisane na kartkach, których znalezienie umożliwi dostęp do systemu, plików lub usług internetowych podejrzanego (na przykład do poczty elektronicznej). Rejestrator DVR (używany do nagrywania programów telewizyjnych) to nośnik, który również może zawierać ważne dowody. Oprogramowanie EnCase firmy opentext umożliwia tworzenie obrazów i analizę plików z rejestratorów DVR. EnCase **tworzy obrazy bitowe**. Tego typu narzędzia generują bit po bicie kopię pierwotnego nośnika, obejmującą pliki oznaczone do usunięcia.

Śledczy musi oczywiście zadbać o to, by pliki będące dowodami zostały zachowane w pierwotnym stanie, w jakim zostały uzyskane. W dalszych rozdziałach stanie się jasne, w jaki sposób informatycy śledczy wykorzystują procesy, sprzęt i oprogramowanie do utrzymania dowodów w wyjściowym stanie.

Typy uzyskiwanych dowodów w informatyce śledczej

Za pomocą informatyki śledczej można uzyskiwać niemal dowolne rodzaje plików — od systemów plików po pliki tworzone przez użytkownika (na przykład arkusze kalkulacyjne). W następnych punktach opisałem najważniejsze typy plików uzyskiwane i wykorzystywane w dochodzeniach. Liczne z tych plików często można odtworzyć nawet w sytuacji, gdy użytkownik je usunął.

Poczta elektroniczna

Poczta elektroniczna jest zapewne najważniejszym typem dowodów elektronicznych. Jest bardzo istotna z kilku powodów. Oto niektóre z nich:

- ustalanie kontroli, własności i zamiarów;
- odtwarzanie łańcucha zdarzeń;
- powszechność;
- trwałość (manipulowanie dowodami);
- dopuszczalność;
- dostępność.

Kontrola, własność i zamiary

W informatyce śledczej ustalenie kontroli, własności i zamiarów jest kluczowe, aby dowód mógł być uznany za obciążający. Czasem żadne dane nie są bardziej osobiste niż poczta elektroniczna. Na jej podstawie można określić zamiary podejrzanego i ofiary. W sprawie zamordowanej przez Roberta Glassa Sharon Lopatki poczta elektroniczna była najważniejszym dowodem w procesie o morderstwo. Glass i Lopatka wymienili między sobą wiele e-maili przed

spotkaniem w Karolinie Północnej, gdzie Glass torturował i udusił Lopatkę. E-maile potwierdziły przerażającą tezę, że tortury i morderstwo miały miejsce za obopólną zgodą.

W sprawach dotyczących posiadania pornografii dziecięcej obrońcy przeważnie utrzymują, że oskarżony nie wiedział, iż materiały znajdowały się w jego komputerze. Oskarżenie musi dowieść, że oskarżony wiedział o istnieniu materiałów i że na zdjęciach znajdowały się osoby nieletnie. Dowody z poczty elektronicznej często pozwalają stwierdzić, że zdjęcia były udostępniane przez podejrzanego innym pedofilom. Ostatecznie pomaga to dowieść winy podsądnego oraz oskarżyć go o posiadanie zdjęć ilustrujących wykorzystywanie dzieci i posługiwanie się komputerem do rozpowszechniania nielegalnych materiałów. Za pomocą procesu haszowania algorytmem MD5 można sprawdzić, czy zdjęcie z jednego komputera jest identyczne ze zdjęciem na innym komputerze.

Łańcuch wydarzeń

Odtwarzanie wydarzeń prowadzących do popełnienia przestępstwa jest ważnym elementem opisu sprawy. Często jeden plik z poczty elektronicznej zawiera wielodniową konwersację i obejmuje godziny, daty, nadawcę oraz odbiorcę wiadomości. Może to pomóc w wyjaśnieniu okoliczności popełnienia przestępstwa.

Powszechność

Poczta elektroniczna jest bardzo ważna, ponieważ tak często służy nam do komunikowania się z innymi osobami. Jest powszechna w komunikacji prywatnej i biznesowej. W śledztwie dotyczącym firmy Enron zebrano i zbadano dziesiątki tysięcy e-maili. Niektóre biura rachunkowe mające dział informatyki śledczej tworzą odrębną jednostkę z grupą analityków, których jedynym zadaniem jest analizowanie dowodów w postaci e-maili.

Trwałość (manipulowanie dowodami)

Manipulowanie dowodami polega na ukrywaniu, niszczeniu, modyfikowaniu lub fałszowaniu dowodów. Jest to istotne naruszenie prawa, uznawane w wielu krajach za poważne przestępstwo. W sprawie Mattel przeciwko MGA Entertainment sędzia okręgowy Stephen Larson orzekł, że ława przysięgłych może wysłuchać zeznań przedstawiciela firmy Mattel. Wedle tych zeznań były pracownik Mattela, Carter Bryant, używał aplikacji Evidence Eliminator do manipulowania dowodami przed udostępnieniem swojego komputera prawnikom w 2004 roku.

Poczta elektroniczna jest bardzo cenna dla śledczych, ponieważ nawet jeśli oskarżony próbuje manipulować przy e-mailach na swoim komputerze, nadal można do nich dotrzeć innymi źródłami. Pliki z e-mailami często znajdują się zarówno na komputerze odbiorcy, jak i na komputerze podejrzanego. Dostawca usług pocztowych może też otrzymać nakaz przekazania plików z e-mailami przechowywanych na serwerach poczty elektronicznej. Pliki z e-mailami często można też pobrać ze smartfonów (na przykład z iPhone'ów) i innych urządzeń, takich jak iPad lub MacBook.

Dopuszczalność

Sędziowie i sądy od lat dopuszczają e-maile jako dowody w sprawach. Co ciekawe, w jednej sprawie, Rombom i inni przeciwko Weberman i inni, sędzia dopuścił jako dowód wydruki e-maili. Powód zeznał, że otrzymał e-maile od pozwanego i je wydrukował.

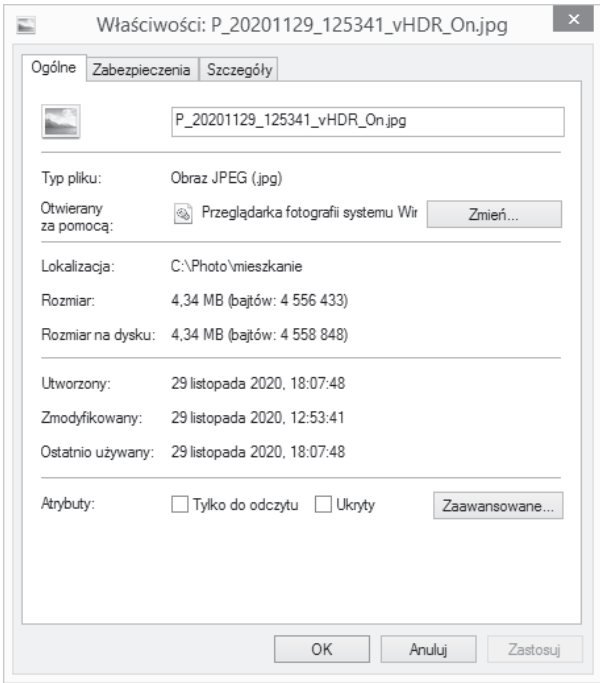
Dostępność

Inaczej niż w przypadku wielu innych źródeł dowodów dostęp do e-maili podejrzanego nie zawsze wymaga nakazu przeszukania. Departament Sprawiedliwości Stanów Zjednoczonych argumentował, że po otwarciu e-mail nie jest już chroniony ustawą o przechowywanej korespondencji (Stored Communications Act — SCA). Choć sędzia już odrzucił rządowy wniosek o przeszukanie bez nakazu, rząd nadal argumentował, że ma prawo do swobodnego dostępu do e-maili, gdy te znajdują się w chmurze. Zgodnie z ustawą SCA przechowywana korespondencja, na przykład e-mail sprzed mniej niż 180 dni, wymaga uzyskania nakazu. Firmy takie jak Yahoo!, Google i Microsoft utworzyły organizację Electronic Frontier Foundation, która stanowczo sprzeciwia się działaniom rządu w omawianym obszarze. Jednak zdaniem niektórych analityków prawo może się zmienić na korzyść rządu.

Mimo to oczywiste jest, że firmowe e-maile pracownika są własnością pracodawcy. Dlatego firma może sprawdzać e-maile pracowników bez ich zgody. W 2009 roku w sprawie Stengart przeciwko Loving Care Agency Wydział Apelacyjny Sądu Najwyższego Stanu New Jersey potwierdził, że pracodawca może otwierać i czytać e-maile pracownika bez jego zgody, jeśli pracownik używa firmowych technologii do dostępu do poczty elektronicznej. Dlatego dostęp do e-maili jest często łatwiejszy niż w przypadku innych metod komunikacji.

Pliki graficzne

Istnieje wiele typów plików graficznych. Najczęściej używane formaty to BMP (bitmapy systemu Windows), JPEG (ang. *Joint Photographic Experts Group*), TIFF (ang. *Tagged Image File Format*) i PNG (ang. *Portable Network Graphics*). Zdjęcia są wyjątkowo istotne w sprawach o wykorzystywanie dzieci. Fotografie są dziś jeszcze ważniejsze niż 20 lat temu, ponieważ zdjęcia cyfrowe zawierają szczegółowe informacje o aparacie użytym do wykonania fotografii (co może dowodzić jego własności) i często obejmują współrzędne **GPS** (ang. *Global Positioning System*), co pozwala ustalić lokalizację urządzenia (na przykład smartfonu) i czas wykonania zdjęcia. Te metadane często są dołączone do fotografii wykonanych za pomocą smartfonu. Zwykle metadane dołączone do zdjęć cyfrowych pozwalają ustalić producenta i model aparatu użytego do wykonania fotografii, co jest cenną informacją dla śledczych. **Metadane pliku** (zobacz rysunek 1.1) to informacje na temat pliku. Mogą obejmować datę utworzenia, modyfikacji i ostatniego dostępu do pliku, a czasem także dane na temat użytkownika, który jest autorem pliku.



RYSUNEK 1.1. Metadane pliku

Większość profesjonalnego oprogramowania do analizy plików graficznych (w tym aplikacja FTK firmy AccessData) ma interfejs użytkownika pozwalający filtrować dane według typów plików i wyodrębniać zdjęcia. Pliki graficzne są grupowane, a oprogramowanie potrafi wydobywać zdjęcia z plików niegraficznych. Na przykład jeśli e-mail lub dokument programu Microsoft Word zawiera zdjęcie, aplikacja potrafi je wyodrębnić i dodać do grupy innych znalezionych plików graficznych.

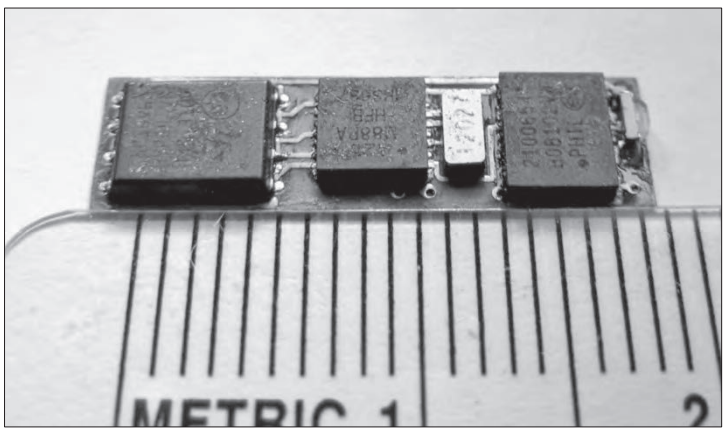
Oprogramowanie X-Ways Forensics i inne narzędzia wspomagające śledczych umożliwiają przefiltrowanie wszystkich zdjęć na podstawie procentu, jaki zajmują na nich odcienie skóry ludzkiej. Dzięki temu po wyszukiwaniu wyświetlane są tylko zdjęcia przedstawiające ludzi. Zdjęcia są wykorzystywane przez organy ścigania i sprawiedliwości od wielu lat. Jednak obecnie zdjęcia cyfrowe zapewniają więcej informacji niż tradycyjne fotografie na kliszach. Wiele serwisów internetowych usuwa metadane ze zdjęć cyfrowych, dlatego śledczy czasem potrzebują nakazu, aby móc uzyskać interesujące ich fotografie w pierwotnym formacie (razem z metadanymi). W rozdziale 11., „Analiza zdjęć", znajdziesz szczegółowe omówienie analizy zdjęć cyfrowych.

Filmy

Dowody w postaci filmów mogą znajdować się w wielu rodzajach urządzeń, w tym w komputerach, kamerach, aparatach fotograficznych i telefonach komórkowych. Nagrania z systemów monitoringu są zwykle przechowywane w komputerach, dlatego też są uwzględniane

w informatyce śledczej. Nagrania z systemów monitoringu często kojarzą się z włamaniami do banków i sklepów, jednak takie filmy wykorzystuje się w znacznie szerszym zakresie spraw kryminalnych.

Skimmery stosowane w bankomatach doprowadziły na całym świecie do kradzieży środków wartych miliony dolarów. **Skimmer** (zobacz rysunek 1.2) jest urządzeniem do przechwytywania danych zapisanych na pasku magnetycznym karty bankomatowej, karty kredytowej lub karty debetowej. Nagrania z systemów monitoringu mogą okazać się kluczowe do schwytania przestępców stosujących skimmery.



RYSUNEK 1.2. Urządzenie do skimmingu

Monitoring wizyjny polega na wykorzystaniu transmitowanego obrazu w określonej lokalizacji. Na przykład w Londynie zamontowanych jest ponad 600 000 kamer monitoringu wizyjnego. Zostały one wykorzystane między innymi w dochodzeniach dotyczących obrabowanych turystów i w głośnych sprawach takich jak otrucie byłego rosyjskiego szpiega Aleksandra Litwinienki w 2006 roku.

Informatycy śledczy dysponują rozmaitymi narzędziami, w tym poprawiającymi jakość analizowanego nagrania. Inne narzędzia na podstawie konfiguracji generują zdjęcia z określonych momentów nagrania. Te zdjęcia są przydatne, ponieważ mogą zostać dołączone do akt. Co ważniejsze, dostępne narzędzia zapewniają śledczym skuteczną technikę identyfikowania, który moment nagrania stanowi ważny dowód obciążający. Dzięki temu nie trzeba oglądać całego filmu. Ponadto jeśli treść nagrania jest wstrząsająca, śledczy nie musi oglądać całości materiału.

Ostatecznie (w sądzie) nagrania wideo mogą okazać się dla ławy przysięgłych najbardziej przekonującym typem dowodów i doprowadzić do skazania przestępcy.

Odwiedzone witryny i wyrażenia wyszukiwane w internecie

W organach ścigania trwają dyskusje nad tym, czy należy odłączyć komputer od zasilania, aby zachować dowody w pierwotnym stanie, czy może jednak komputer powinien pozostać włączony po jego znalezieniu. Z powodu postępów w szyfrowaniu i natury dowodów, które

mogą zostać utracone po wyłączeniu urządzenia, większość śledczych uważa, że należy zbadać system, póki jest on włączony. **Szyfrowanie** to proces przekształcania tekstu na nieczytelny format za pomocą matematycznego wzoru nazywanego algorytmem. Pliki i dane dowodowe związane z przeszukiwaniem internetu i odwiedzonymi witrynami są łatwiej dostępne, dopóki komputer jest włączony. Dzieje się tak, ponieważ duża część działań użytkownika, w tym jego aktywność w internecie, jest przechowywana w pamięci RAM (ang. *Random Access Memory*). Jest ona często nazywana pamięcią krótkotrwałą, gdyż po wyłączeniu komputera jej zawartość znika. Należy zauważyć, że w momencie odwiedzania witryny komputer kliencki kieruje żądanie do serwera WWW. Komputer kliencki pobiera z witryny dokument HTML i powiązane zasoby (na przykład zdjęcia) i umieszcza je w pamięci.

Na rysunku 1.3 **komputer kliencki** to maszyna żądająca zasobu z serwera. Głównym zadaniem **serwera WWW** jest udostępnianie dokumentów HTML i powiązanych zasobów (na przykład zdjęć) w odpowiedzi na żądania klienta. Najłatwiejszy sposób na zapamiętanie ról komputera klienckiego i serwera to wyobrażenie sobie komputera jako klienta, a serwera jako dostawcy usług. Większość profesjonalnych narzędzi informatyki śledczej potrafi skutecznie zarejestrować zawartość pamięci RAM, gdy komputer jest włączony. Dostępnych jest też wiele bezpłatnych narzędzi do analizy pamięci RAM.

RYSUNEK 1.3. Komunikacja między klientem a serwerem WWW

Analiza śledcza telefonów komórkowych

Dziedzina analizy śledczej telefonów komórkowych (nazywana też analizą śledczą urządzeń mobilnych) szybko się rozwija wraz ze wzrostem możliwości takich urządzeń. Telefon komórkowy potrafi ustalić, kogo podejrzany zna (kontakty), z kim się spotyka (kalendarz), z kim rozmawiał (rejestry rozmów) i co mówił (wiadomości tekstowe). Inne urządzenia mobilne mogą zapewniać dowody w postaci zdjęć i filmów (aparat i kamera w urządzeniu) czy informacji pozwalających ustalić odwiedzone miejsca (odbiornik GPS) albo dokonane zakupy internetowe i odwiedzone witryny (smartfony z obsługą internetu).

Telefony komórkowe często wykorzystuje się do namierzania podejrzanych. W śledztwie w sprawie morderstwa Freda Jablina detektyw Coby Kelley uzyskał nakaz udostępnienia rejestrów lokalizacji telefonu komórkowego podejrzanej Piper Rountree. Ponieważ wieże telekomunikacyjne rejestrują telefon komórkowy użytkownika, gdy ten przemieszcza się z jednej komórki (z jednego obszaru) do innej, detektyw mógł zlokalizować podejrzaną, kiedy poruszała się na wschód drogą I-64 w kierunku lotniska Norfolk. Później wykryto transmisję z tego samego telefonu z Baltimore w stanie Maryland. W toku dalszego śledztwa ustalono,

że Rountree zarezerwowała lot z Baltimore do Teksasu, posługując się imieniem siostry. Piper Rountree utrzymywała, że nigdy nie opuściła Houston w Teksasie, jednak rejestry dotyczące jej telefonu komórkowego były dowodem na nieprawdziwość tych twierdzeń i pozwoliły uznać ją za winną.

Więcej informacji na temat wykorzystania telefonów komórkowych w informatyce śledczej znajdziesz w rozdziale 9., „Analiza śledcza urządzeń mobilnych".

Analiza śledcza urządzeń IoT

W ostatnich latach nastąpił znaczny rozwój dostępnych w domach systemów wykorzystujących sztuczną inteligencję. Urządzeniami wykorzystującymi sztuczną inteligencję można sterować za pomocą smartfonów. Takie urządzenia można też integrować z innymi inteligentnymi urządzeniami — od termostatu, przez system monitoringu domu, po oświetlenie. Dlatego wiedza o nowych ekosystemach narzędzi i pozostawianych przez nie (lokalnie lub w chmurze) śladach cyfrowych jest bardzo istotna dla informatyków śledczych. Analiza śledcza urządzeń IoT jest opisana szczegółowo w rozdziale 14., „Analiza śledcza urządzeń IoT i nowe technologie".

Jakie umiejętności powinien posiadać informatyk śledczy?

Warto zauważyć, że informatyka śledcza to dziedzina multidyscyplinarna. Wykorzystuje się w niej umiejętności z obszarów informatyki, prawa materialnego i procesowego, kryminologii, matematyki, komunikacji i lingwistyki.

Wiedza z obszaru informatyki

W dziedzinie informatyki ważna jest solidna wiedza z zakresu systemów operacyjnych i używanych w nich systemów plików. Dobre podstawy z tej dziedziny pozwolą śledczemu ustalić, gdzie pliki są przechowywane, a także ocenić ich wartość dla prokuratorów w sprawach karnych. Znajomość systemów operacyjnych pomaga zrozumieć interakcje między sprzętem i oprogramowaniem. Jest to niezbędne do odtworzenia poczynań użytkownika komputera. Na przykład **BitLocker**, narzędzie szyfrujące wprowadzone w wersjach Ultimate i Enterprise systemu Microsoft Windows Vista, umożliwia szyfrowanie plików, katalogów i napędów. Wyłączenie komputera z włączonym narzędziem BitLocker uruchamia proces szyfrowania. Świadomy tego informatyk śledczy po natrafieniu na ów system operacyjny we włączonym komputerze będzie wiedział, czym grozi wyłączenie maszyny.

Samo zlokalizowanie i pobranie plików dowodowych nie wystarczy. Doświadczony informatyk śledczy musi posiadać rozbudowane umiejętności dochodzeniowe, które pozwolą mu powiązać dowody z określoną osobą. Taki śledczy powinien umieć wykorzystać dowody elektroniczne do wykazania kontroli, własności i zamiarów podejrzanego. Musi na przykład umieć udowodnić, że podejrzany kontrolował komputer w czasie, gdy pliki były zapisywane w pamięci. W tym scenariuszu dowodem może być to, że użytkownik posłużył się loginem

i hasłem do uzyskania dostępu do komputera. Własność jest następnym ważnym czynnikiem przy dowodzeniu winy. Własności można dowieść, jeśli śledczy potrafi wykazać, że podejrzany utworzył plik, zmodyfikował go lub przesłał e-mailem do innej osoby. Ponadto do skazania przestępcy zwykle niezbędne jest udowodnienie zamiaru. W informatyce śledczej oskarżony może utrzymywać, że nie zamierzał odwiedzić określonej witryny lub że przypadkowo pobrał zdjęcia, ale nigdy ich nie oglądał. Dlatego informatyk śledczy w celu udowodnienia zamiaru musi wykazać, że witryna została odwiedzona wielokrotnie lub że zdjęcie było oglądane w różnych okolicznościach i później zostało udostępnione innym.

Wiedza z zakresu prawa

Wiedza prawna jest niezwykle ważna, zwłaszcza jeśli chodzi o informatykę śledczą. Pierwszym wyzwaniem dla śledczego może być dostęp do komputera podejrzanego. Jeśli komputer podejrzanego jest zlokalizowany w jego mieszkaniu, konieczna jest znajomość czwartej poprawki do Konstytucji Stanów Zjednoczonych. Poprawka ta dotyczy rewizji i zatrzymań. Aby uzyskać dostęp do komputera, śledczy muszą przekonać sędziego, że zostało popełnione przestępstwo i że istnieją uzasadnione podejrzenia, iż w danym miejscu znajduje się ważny dowód. Organy ścigania muszą uprawdopodobnić winę lub przedstawić uzasadnione podstawy do przeszukania.

Umiejętności komunikacyjne

W dziedzinie informatyki śledczej nie wolno lekceważyć umiejętności pisania. Śledczy musi udokumentować proces dochodzeniowy i swoje ustalenia. Ponadto raport musi zostać napisany w taki sposób, aby zaangażowane w sprawę osoby, które nie posiadają wiedzy technicznej analityka od informatyki śledczej, potrafiły zrozumieć wnioski. Jeśli sprawa karna trafi do sądu, informatyk śledczy może zostać powołany jako biegły sądowy. Musi wtedy precyzyjnie przekazać swoje ustalenia sędziemu i ławie przysięgłych, a osoby te mogą posiadać niewielką wiedzę na temat komputerów i informatyki śledczej.

Znajomość języków

Obecnie przestępstwa częściej mają zasięg międzynarodowy — po części z powodu powszechności internetu. Nasilenie się cyberprzestępczości i wykorzystywanie nowych technologii przez międzynarodowych terrorystów sprawiają, że rośnie zapotrzebowanie na śledczych znających języki obce. Dlatego w niektórych dochodzeniach bardzo przydatni mogą okazać się informatycy śledczy posługujący się innymi językami.

Nieustanne kształcenie się

Skuteczny informatyk śledczy stale pogłębia i aktualizuje wiedzę oraz zdobywa nowe umiejętności. Niektóre z nich są bardzo istotne, ale trudne do zmierzenia. Umiejętność abstrakcyjnego i niekonwencjonalnego myślenia są niezbędne, ponieważ każde przestępstwo jest

inne i wiąże się z odmiennymi dowodami. Dlatego informatycy śledczy muszą nieustannie opracowywać nowe techniki i rozwiązania. Łatwość dostosowywania się do zmian i ciągłego uczenia się są ważne zwłaszcza w kontekście błyskawicznego rozwoju technologii. Szybkie zmiany technologiczne skutkują też nowymi rodzajami przestępstw. Trudne w pomiarze są też umiejętności psychologiczne. Umiejętność zrozumienia przestępcy pozwala lepiej zrozumieć działania danej osoby i szybko znajdować odpowiedzi w trakcie dochodzenia. Z tego powodu jest zapotrzebowanie na ekspertów, którzy potrafią opracować profile seryjnych morderców i innych przestępców.

Programowanie

Choć informatyk śledczy nie musi dobrze znać się na programowaniu, pewne umiejętności z tego zakresu mogą być przydatne. Oto kilka konkretnych przykładów: znajomość systemu Linux może pomóc śledczemu w pracy z serwerami opartymi na tym systemie, klonowaniu dysków, analizie urządzeń z systemem Android, analizie aplikacji z systemu Android i badaniu sieci; skrypty AppleScript można wykorzystać do sczytywania zawartości witryn lub łamania kodów PIN w komputerach firmy Apple; język Python można zastosować do zautomatyzowanego sczytywania zawartości witryn; EnScripts to konfigurowalne skrypty, które mogą stosować użytkownicy narzędzia EnCase; *cmdlety* i skrypty powłoki PowerShell umożliwiają pobieranie kluczowych dowodów z różnych systemów operacyjnych, w tym z systemu Windows.

Poufność

Niezwykle ważna jest też umiejętność zachowania poufności informacji. Należy przekazywać je wyłącznie osobom, które muszą posiadać informacje o dochodzeniu, a im mniej jest takich ludzi, tym lepiej. Jeśli podejrzany dowie się o ustaleniach śledczych, grozi to jego ucieczką i zniszczeniem dowodów, czyli ukryciem, zmodyfikowaniem lub uszkodzeniem dowodów. Niekorzystne są też wycieki informacji do mediów, a w głośnych sprawach media mogą wpływać na opinie ławy przysięgłych.

Znaczenie informatyki śledczej

Znaczenie informatyki śledczej rośnie, ponieważ coraz więcej aspektów ludzkiego życia jest zapisywanych za pomocą technologii. Informacje o naszym życiu są rejestrowane w komputerach, telefonach komórkowych i sieci WWW (przede wszystkich w serwisach społecznościowych). Na przykład Facebook ma blisko dwa miliardy użytkowników i zapewnia śledczym mnóstwo informacji — od zdjęć, przez wskazówki dotyczące haseł, po sieci znajomych (potencjalnych wspólników) podejrzanego.

Śledczy zwykle muszą odtworzyć wydarzenia prowadzące do przestępstwa. Technologia to ułatwia. Podejrzanego można namierzyć za pomocą karty MTA MetroCard używanej w nowojorskim metrze (powiązanej z kartą kredytową) lub na podstawie płatności w systemie E-Z Pass. Na początku 2014 roku prokuratorzy hrabstwa Queens w stanie Nowy Jork oskarżyli taksówkarza Rodolfo Sancheza o kradzież mienia o dużej wartości, kradzież usług

i posiadanie kradzionego mienia. Stało się tak, gdyż nadajnik i rejestry systemu E-Z Pass wykazały, że kierowca unikał opłat za liczne mosty i tunele będące pod zarządem MTA (Metropolitan Transportation Authority). Podejrzanego można też łatwo śledzić na podstawie użytkowania telefonu komórkowego.

Możliwości kariery

Amerykański Urząd Statystyki Pracy uznał znaczenie informatyki śledczej i bezpieczeństwa teleinformatycznego. Zgodnie z szacunkami tej agencji w latach 2018 – 2028 roku liczba stanowisk w branży informatycznej wzrośnie o 12%. Oznacza to powstanie około 546 200 nowych miejsc pracy. Rosnąca liczba stanowisk po części wynika z reakcji na przestępczą działalność w internecie: kradzieże tożsamości, rozsyłanie spamu, nękanie e-mailami i nielegalne pobieranie materiałów chronionych prawem autorskim.

Miejsca pracy związane z informatyką śledczą powstają w organach ścigania na różnych poziomach: lokalnym, krajowym i międzynarodowym. Jednak także sektor prywatny oferuje wiele stanowisk dla specjalistów od informatyki śledczej. Większość dużych biur rachunkowych posiada laboratorium informatyki śledczej, a największe spośród nich mają kilka takich jednostek w różnych miejscach kraju. Korporacje często korzystają w swoich dochodzeniach z usług działów informatyki śledczej firm rachunkowych. Duża część działalności takich działów dotyczy procesu **eDiscovery** (ang. *electronic discovery*), polegającego na odzyskiwaniu danych cyfrowych. Odzyskiwanie danych może być konieczne na przykład z powodu sporu z inną korporacją lub żądania informacji z komisji SEC (Securities and Exchange Commission). Usługi z obszaru eDiscovery dotyczą zwykle spraw cywilnych.

Specjaliści od informatyki śledczej mogą też znaleźć zatrudnienie w prywatnych agencjach detektywistycznych. Takie firmy (na przykład CODEDETECTIVES LLC) często są angażowane przez strony postępowania cywilnego, na przykład w sprawach rozwodowych, gdy występuje podejrzenie niewierności, a zwłaszcza kiedy trwa walka o prawo do opieki nad dziećmi. Zdaniem niektórych rozwój informatyki śledczej to rezultat działań zmierzających do dowiedzenia niewierności partnera.

Wraz ze wzrostem znaczenia informatyki śledczej i pojawianiem się nowych technologii rośnie też potrzeba powstawania nowego oprogramowania i sprzętu. Producenci, na przykład AccessData, opentext, Cellebrita i Paraben, zatrudniają pracowników znających się zarówno na informatyce, jak i na dochodzeniach. Także niektóre duże kancelarie prawne wraz ze wzrostem zapotrzebowania zatrudniają informatyków śledczych lub korzystają z usług konsultantów z tej dziedziny. Ponadto często się zdarza, że specjaliści od informatyki śledczej są powoływani jako biegli sądowi w postępowaniach karnych i cywilnych.

Systemy finansowe na całym świecie są w dużym stopniu oparte na komunikacji elektronicznej i na cyfrowym przechowywaniu danych o kontach bankowych klientów. Oszustwa związane na przykład z kartami kredytowymi czy przelewam i szybko zmusiły instytucje finansowe do inwestycji w dziedzinie informatyki śledczej, aby umożliwić ujęcie i skazanie przestępców.

Dzięki temu instytucje finansowe mają większą wiedzę na temat działań przestępców, a także strategii i technik zwiększających bezpieczeństwo komputerów.

Oto inne organizacje zatrudniające specjalistów od informatyki śledczej i korzystające z ich usług: agencje Departamentu Obrony Stanów Zjednoczonych (w tym wojska lotnicze, wojska lądowe i marynarka wojenna), urząd podatkowy (jest to jedna z agencji rządowych, która najwcześniej zaczęła korzystać z informatyki śledczej), agencje federalne (FBI, DHS, ICE, DEA i U.S. Secret Service posiadają laboratoria informatyki śledczej). Jeśli chodzi o FBI, informacje zdobywane za pomocą informatyki śledczej są niezbędne niezależnie od tego, czy dochodzenie dotyczy „przestępczości białych kołnierzyków", na przykład prania pieniędzy, czy elektronicznej komunikacji między terrorystami z Al-Kaidy. Także agencja Secret Service coraz częściej posługuje się informatyką śledczą w swoich dochodzeniach (na przykład dotyczących fałszerstwa).

W październiku 2001 roku prezydent Bush podpisał ustawę USA PATRIOT (H.R. 3162). Jeden z jej zapisów dotyczył utworzenia ogólnokrajowych służb ECTF (Electronic Crimes Task Forces). Miały one składać się z federalnych, stanowych i lokalnych organów ścigania, pracowników naukowych i jednostek prywatnych. Te służby odpowiadają za ochronę kluczowej infrastruktury Stanów Zjednoczonych. Ponadto wiedza specjalistów od informatyki śledczej jest niezbędna do skutecznej analizy ataków na krytyczną infrastrukturę, w tym na system finansowy i sieć energetyczną.

Widać więc, że miejsca pracy dla specjalistów od informatyki śledczej są dostępne w wielu branżach, co wynika z cyfryzacji informacji o naszym życiu. Kradzieże takich informacji i ataki na krytyczną infrastrukturę będą się nasilać, co oznacza stałe zapotrzebowanie na ekspertów od informatyki śledczej. Zakres tej dziedziny poszerzył się w tak znacznym stopniu, że pojawiły się wyspecjalizowane stanowiska. Niektóre osoby są ekspertami od konfiskowania urządzeń cyfrowych i tworzenia zgodnie z prawem ich obrazów. Te obrazy są następnie przekazywane do innego miejsca w laboratorium, gdzie są przeszukiwane pod kątem plików powiązanych z dochodzeniem. Później inny zespół może odpowiadać za pisanie raportu i udostępnianie dowodu w zabezpieczonej witrynie. Ten ostatni krok umożliwia przeglądanie dowodów obrońcom i prokuratorom.

Specjalizacja w dziedzinie informatyki śledczej jest widoczna także w związku z różnymi rodzajami urządzeń. Na przykład śledczy przeprowadzający analizę śledczą urządzeń mobilnych koncentrują się na dowodach z telefonów komórkowych, a specjaliści od urządzeń z systemem macOS badają głównie komputery i urządzenia firmy Apple (na przykład iPady i iPody).

Historia informatyki śledczej

Informatyka śledcza pierwotnie powstała na potrzeby badania przestępstw komputerowych. W latach 50., 60. i 70. działali phreakerzy, którzy za pomocą różnych technik wykonywali bezpłatne rozmowy międzymiastowe i międzynarodowe. Steve Jobs i Steve Wozniak, założyciele firmy Apple, podobno sprzedawali urządzenie, które dzięki sztuczkom telekomunikacyjnym umożliwiało użytkownikom wykonywanie bezpłatnych rozmów. Phreakerów czasem uważa się za pierwszych hakerów i za źródło inspiracji dla hakerów komputerowych z lat 80.

Lata 80. — pojawienie się komputerów osobistych

Choć przestępstwa związane z komputerami są popełniane od wielu lat, na dużą skalę zaczęły się nasilać wraz z pojawieniem się w latach 80. komputerów osobistych. Pionierem w tej branży była firma IBM, która w 1981 roku wprowadziła na rynek komputer 5150 PC. W latach 80. IBM konkurował z innymi producentami komputerów osobistych, takimi jak Atari, Commodore, Tandy i Apple. W tym okresie Apple odnosił duże sukcesy na rynku komputerów osobistych. W 1984 roku wprowadził na rynek komputer Macintosh 128K z wbudowanym czarno-białym wyświetlaczem. W tym samym roku firma zaczęła sprzedaż komputera Macintosh 512K. Ten komputer obsługiwał oprogramowanie biznesowe, w tym Microsoft Excel. Wprowadzony w 1987 roku komputer Macintosh SE stał się jednym z najpopularniejszych komputerów osobistych swoich czasów. Ciekawe jest to, że w tym samym czasie pojawiły się pierwsze elektroniczne tablice ogłoszeniowe, które ułatwiły komunikację między hakerami. W efekcie powstały grupy hakerskie takie jak amerykańska Legion of Doom. W filmie *Gry wojenne* z 1983 roku przedstawiono widzom pomysł użycia przez hakerów komputera osobistego do uzyskania dostępu do komputerów rządowych. W 1984 roku Eric Corley (używający pseudonimu Emmanuel Goldstein) zaczął publikować kwartalnik „2600: The Hacker Quarterly",umożliwiający hakerom wymianę pomysłów. Kevin Mitnick, jeden z pierwszych hakerów, został w 1989 roku skazany za kradzież oprogramowania firmware firmy DEC i kodów dostępu do sieci MCI. Na fali licznych głośnych włamań do systemów amerykański Kongres uchwalił w 1986 roku ustawę o oszustwach i nadużyciach komputerowych (Computer Fraud and Abuse Act). Później kilkakrotnie wprowadzono poprawki do tej ustawy.

FBI

W 1984 roku FBI utworzyło jednostkę Magnetic Media Program, znaną później jako **CART** (Computer Analysis and Response Team). Odpowiadała ona za dochodzenia z zastosowaniem informatyki śledczej. Agent specjalny Michael Anderson z wydziału dochodzeń karnoskarbowych amerykańskiego urzędu skarbowego jest czasem nazywany „ojcem informatyki śledczej".

NCMEC

W amerykańskich organach ścigania na poziomie lokalnym informatycy śledczy zwykle poświęcają dużo czasu na sprawy, w których ofiarami są dzieci, głównie związane z posiadaniem i rozpowszechnianiem pornografii dziecięcej. W 1984 roku amerykański Kongres utworzył jednostkę **NCMEC** (National Center for Missing and Exploited Children). Ma ona pomagać w znajdowaniu zaginionych dzieci i walczyć z wykorzystywaniem (seksualnym) nieletnich. Jednostka ta prowadzi też centralny rejestr przestępstw przeciwko dzieciom.

Lata 90. — wpływ internetu

Wraz z pojawieniem się w latach 90. przeglądarek internetowych (takich jak Netscape) dostęp do internetu stał się dużo łatwiejszy. Nie trzeba już było używać wiersza poleceń, aby otworzyć zasoby internetowe. Zamiast tego można było korzystać z wygodnego i atrakcyjnego wizualnie interfejsu. Przeglądarki internetowe doprowadziły do masowego użytkowania

internetu za pomocą komputerów. Ważne było też to, że maszyny, które wcześniej nie mogły się ze sobą komunikować (na przykład komputery PC i komputery Mac), teraz mogły robić to w stosunkowo prosty sposób dzięki opracowaniu wspólnego protokołu do komunikacji w internecie — HTTP (ang. *HyperText Transport Protocol*). W tym czasie powstała też poczta elektroniczna, choć początkowo służyła do komunikowania się w ramach organizacji. Dzięki sieciom e-mailowym międzynarodowe firmy radykalnie ograniczyły koszty rozmów telefonicznych. Nowe zastosowania technologii komunikacyjnych spowodowały, że większe znaczenie zaczęto przypisywać dowodom elektronicznym. W 1993 roku miała miejsce pierwsza międzynarodowa konferencja poświęcona dowodom komputerowym.

Amerykański Departament Obrony

Wydana w 1998 roku dyrektywa DRI #27 nakazywała amerykańskim siłom powietrznym utworzenie wspólnego Laboratorium Informatyki Śledczej Departamentu Obrony. Jednostka ta miała odpowiadać za kontrwywiad oraz dochodzenia karne i pozyskiwanie dowodów komputerowych. Jednocześnie opracowano program szkoleń z zakresu informatyki śledczej (Defense Computer Investigations Training Program). Ten program szkoleniowy doprowadził do powstania akademii, która później otrzymała akredytację Amerykańskiej Rady ds. Edukacji (American Council of Education). Jednostka DC3 (Department of Defense Cyber Crime Center) została utworzona na podstawie tej akademii i wspomnianego wcześniej laboratorium, a w 2002 roku dołączono do niej instytut DCCI (Department of Defense Cyber Crime Institute). DC3 współpracowało z centrum CTANS (Center for Telecommunications and Network Security) z Uniwersytetu Stanu Oklahoma nad utworzeniem i prowadzeniem repozytorium NRDFI (National Repository for Digital Forensic Intelligence). Owocem tej współpracy są różne narzędzia z dziedziny informatyki śledczej.

Amerykański urząd podatkowy

Początki amerykańskiego urzędu podatkowego sięgają wojny secesyjnej, kiedy to prezydent Lincoln powołał naczelnika urzędu skarbowego. Obecnie urząd podatkowy jest jednostką Departamentu Skarbu. Wraz ze wzrostem popularności komputerów rośnie też potrzeba stosowania informatyki śledczej w dochodzeniach prowadzonych przez urząd podatkowy. Agencja IRS-CID (IRS Criminal Investigation Division) w ramach programu Electronic Crimes Program zleciła Elliottowi Spencerowi opracowanie narzędzia do informatyki śledczej o nazwie ILook. Agencja zaczęła korzystać z tego narzędzia w 2000 roku, aby usprawnić dochodzenia w sprawach finansowych. Pakiet ILook Suite był bezpłatnie dostępny dla lokalnych i stanowych organów ścigania.

Amerykańska agencja Secret Service

Często uważa się, że United States Secret Service (USSS) zajmuje się wyłącznie ochroną najwyższego zwierzchnika sił zbrojnych, którym jest prezydent Stanów Zjednoczonych. Jednak ta agencja federalna ma stosunkowo długą i wyjątkową historię działań w dziedzinie informatyki śledczej. Wynika to z tego, że agenci operacyjni USSS uczestniczą w dochodzeniach w całych Stanach Zjednoczonych, w tym w sprawach dotyczących prania i fałszowania pieniędzy.

W ustawie o przestępczości z 1994 roku Kongres upoważnił USSS do stosowania informatyki śledczej i wiedzy technicznej w dochodzeniach karnych dotyczących zaginionych i wykorzystywanych dzieci. Dlatego USSS ściśle współpracuje z NCMEC. W 1996 roku USSS utworzyła jednostkę **ECTF** (Electronic Crimes Task Force), odpowiedzialną za dochodzenia w sprawie cyberprzestępstw prowadzone razem z innymi służbami.

W ustawie USA PATRIOT z 2001 roku upoważniono USSS do rozbudowania odnoszącej sukcesy nowojorskiej jednostki ECTF i objęcia jej działalnością całego kraju. Rok później, w reakcji na brak koordynacji agencji przed wydarzeniami z 11 września 2001 roku, utworzono Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych. Głównym zadaniem tej agencji jest ochrona Stanów Zjednoczonych przed atakami terrorystycznymi i skuteczne reagowanie na klęski żywiołowe. USSS zostało agencją działającą w ramach Departamentu Bezpieczeństwa Wewnętrznego. W kwietniu 2003 roku ustawa PROTECT (nazywana też ustawą Amber Alert) dała USSS pełne uprawnienia do zarządzania dochodzeniami dotyczącymi nadużyć wobec dzieci oraz zapewniła w tym celu dodatkowe fundusze i zasoby. W 2007 roku agencja utworzyła instytut NCFI (National Computer Forensics Institute), prowadzony wspólnie przez USSS, Departament Bezpieczeństwa Wewnętrznego, zrzeszenie prawników okręgu Alabama, stan Alabama i miasto Hoover w stanie Alabama. NCFI prowadzi szkolenia z zakresu informatyki śledczej dla organów ścigania i wymiaru sprawiedliwości. W budynku NCFI znajdują się sale z zaawansowanymi technologicznie urządzeniami, laboratorium informatyki śledczej i zaaranżowana sala sądowa. W praktyce USSS zwykle w mniejszym stopniu angażuje się w sprawy dotyczące wykorzystywania dzieci, ponieważ koncentruje się na przestępstwach finansowych. FBI, DHS-ICE i Postal Inspection Service są bardziej aktywne w takich sprawach.

Konieczność współpracy międzynarodowej, zwłaszcza z organami ścigania w Europie, zyskała na znaczeniu po wydarzeniach z 11 września 2001 roku. W 2009 roku USSS utworzyła pierwszą jednostkę European Electronic Crimes Task Force z siedzibą w Rzymie. Rok później USSS utworzyła analogiczną jednostkę w Wielkiej Brytanii.

Współpraca międzynarodowa

Współpraca międzynarodowa organów ścigania jest niezwykle ważna, ponieważ zwykle im poważniejsze przestępstwo, tym większy jego zasięg geograficzny. Przestępcy często posługują się internetem do komunikowania się na poziomie międzystanowym i międzynarodowym. W 1995 roku utworzono organizację IOCE (International Organization on Computer Evidence). Wspomaga ona wymianę informacji między organami ścigania z różnych państw. W 1998 roku grupa G8 wyznaczyła IOCE do opracowania standardów postępowania z dowodami elektronicznymi.

INTERPOL

Jeśli chodzi o międzynarodowe działania i współpracę, **INTERPOL** odgrywa główną rolę w zakresie wykorzystywania dowodów elektronicznych w dochodzeniach w sprawach karnych. Jest największą na świecie międzynarodową organizacją policyjną. Należy do niej 188 państw.

W 1989 roku sekretariat generalny organizacji został przeniesiony do Lyonu we Francji. W 2004 roku otwarto biuro łącznikowe INTERPOL-u przy Organizacji Narodów Zjednoczonych, a w 2008 roku został wyznaczony mający siedzibę w Brukseli specjalny reprezentant przy Unii Europejskiej.

Zespół reagowania na incydenty INTERPOL-u wspomagał wiedzą z zakresu informatyki śledczej wiele głośnych międzynarodowych dochodzeń. Według raportu z 2008 roku informatycy śledczy z organów ścigania z Australii i Singapuru na prośbę władz kolumbijskich zbadali 609 GB danych z ośmiu laptopów, dwóch zewnętrznych dysków twardych i trzech pamięci USB. Ten sprzęt i zainstalowane oprogramowanie należały do FARC (Fuerzas Armadas Revolucionarias de Colombia), kolumbijskiej antyrządowej organizacji terrorystycznej finansowanej w dużej części ze środków pochodzących z przemytu narkotyków (przede wszystkim kokainy). Kolumbijscy śledczy skontaktowali się z INTERPOL-em w kwestii zbadania skonfiskowanych laptopów, aby niezależni eksperci przyjrzeli się dowodom elektronicznym i potwierdzili twierdzenia rządu, wedle którego dowody były przechowywane w sposób zgodny z przepisami prawa i zasadami zawodowymi.

W 2008 roku zgromadzenie generalne ICPO-INTERPOL w Sankt Petersburgu zatwierdziło powołanie w ramach INTERPOL-u jednostki Computer Forensics Analysis Unit. Jednostka ta prowadzi szkolenia i wspomaga dochodzenia z użyciem informatyki śledczej. Ma też za zadanie tworzyć międzynarodowe standardy poszukiwania, gromadzenia i analizy dowodów elektronicznych.

INTERPOL od lat działa na rzecz zwalczania przestępstw przeciwko dzieciom. Od 2001 roku INTERPOL, podobnie jak NCMEC, prowadzi bazę wykorzystywanych dzieci: ICAID (INTERPOL Child Abuse Image Database). W 2009 roku baza ta została zastąpiona bazą ICSE DB (International Child Sexual Exploitation Image Database), która jest dostępna w czasie rzeczywistym dla organów ścigania z całego świata. Jest to rozbudowana baza z oprogramowaniem do porównywania obrazów pozwalająca łączyć ofiary z miejscami. INTERPOL współpracuje też z innymi agencjami z całego świata, w tym z CIRCAMP (COSPOL Internet Related Child Abuse Material Project) i Virtual Global Taskforce, zwalczając nadużycia wobec dzieci. CIRCAMP to europejska sieć organów ścigania zajmująca się monitorowaniem internetu w celu wykrywania wykorzystywania dzieci. Virtual Global Taskforce ma podobne zadania i misję, ale jest globalną siecią agencji zwalczających nadużycia wobec dzieci w internecie.

INTERPOL z powodzeniem koordynuje międzynarodowe działania w zakresie ścigania osób podejrzanych o pedofilię. W 2006 roku w wyniku policyjnej obławy na internetowych pedofilów w Norwegii śledczy ujawnili laptop z prawie 800 przerażającymi zdjęciami chłopców. Prawie sto spośród fotografii przedstawiało białego mężczyznę w średnim wieku obserwującego wykorzystywanie tych chłopców. Władze poprosiły INTERPOL o pomoc w ustaleniu tożsamości i ujęciu pedofila. INTERPOL rozpoczął wtedy szeroko zakrojoną akcję i za pośrednictwem mediów zwrócił się o pomoc do społeczeństwa. W ciągu 48 godzin od tego komunikatu INTERPOL we współpracy z ICE (Immigration and Customs Enforcement) aresztował 60-letniego Wayne'a Nelsona Corlissa z Union w stanie New Jersey.

Laboratorium RCFL

W 1999 roku w San Diego w stanie Kalifornia utworzono pierwsze laboratorium RCFL (Regional Computer Forensics Laboratory). W 2000 roku w Dallas w stanie Teksas otwarto drugą taką placówkę. RCFL jest finansowanym przez FBI laboratorium, gdzie funkcjonariusze organów ścigania szkolą się w stosowaniu narzędzi informatyki śledczej. Laboratoria te są też wykorzystywane przez urzędników różnych agencji współpracujących w dochodzeniach w sprawach karnych. Mniejsze agencje często nie mają budżetu ani innych zasobów, by stworzyć skuteczne laboratorium informatyki śledczej. Placówki RCFL umożliwiają mniejszym wydziałom policji skierowanie jednego lub dwóch funkcjonariuszy do laboratorium w celu przeszkolenia lub pracy nad śledztwem. Analizowane przestępstwa to terroryzm, pornografia dziecięca, kradzież lub zniszczenie własności intelektualnej, przestępstwa w internecie oraz oszustwa. Obecnie w Stanach Zjednoczonych działa 14 laboratoriów RCFL, a w Europie są dwie takie placówki.

Centra informacyjne

Powołane w 2003 roku amerykańskie centra informacyjne są centralnymi magazynami do zbierania na poziomie stanowym i lokalnym informacji służących zapobieganiu atakom terrorystycznym. Jest to wspólny projekt Departamentu Bezpieczeństwa Wewnętrznego i Departamentu Sprawiedliwości. W Stanach Zjednoczonych istnieje ponad 70 takich centrów informacyjnych. Ich lokalizacje były tajne, jednak grupa Public Intelligence ujawniła umiejscowienie większości placówek. Budynki centrów nie mają oznaczeń ani numeru — podany jest tylko numer skrzynki pocztowej. Na przykład centrum informacyjne zlokalizowane w West Trenton w stanie New Jersey ma numer skrzynki pocztowej 7086 zamiast numeru budynku.

Po wydarzeniach z 11 września w raportach stwierdzono, że brak wymiany informacji między agencjami rządowymi (takimi jak NSA, CIA i FBI) był głównym problemem, który uniemożliwił zapobieżenie atakom terrorystycznym. Na przykład Ziad Jarrah porwał 11 września 2001 roku samolot linii United Airlines odbywający lot 93. Maszyna rozbiła się tego dnia w Pensylwanii. Dwa dni wcześniej, 9 września 2001 roku, Jarrah został zatrzymany przez lokalną policję za przekroczenie prędkości. Policjant z tego patrolu nie posiadał informacji, które pozwoliłyby zatrzymać Jarraha, nie wiedział też, że Jarrah był poszukiwany przez FBI.

Lokalne organy ścigania rejestrują potrzebne informacje, a następnie przekazują je do centrów informacyjnych. Zapisywane informacje obejmują nagrania z kamer monitoringu, numery rejestracyjne samochodów i raporty o podejrzanej aktywności. Owe raporty obejmują doniesienia o osobach robiących zdjęcia obiektów rządowych, rysujących mapy lub odbywających nietypowe spotkania.

Centra informacyjne przechowują bazy danych z informacjami o niemal wszystkich mieszkańcach Stanów Zjednoczonych, w tym o zastrzeżonych numerach telefonów komórkowych, prawach jazdy i roszczeniach ubezpieczeniowych. Rejestrują też materiały ze stosunkowo nieznanych podmiotów zajmujących się eksploracją danych, na przykład z firmy Entersect. Entersect udostępnia działom kadr dane na temat potencjalnych pracowników: rejestry karne, referencje od pracodawców czy informacje o sprawach sądowych, bankructwach i wykształceniu.

Oferuje też usługę dla organów ścigania: Entersect Police Online. Według witryny (*http://entersect.net*) firma zapewnia organom ścigania dostęp przez internet do miliardów zapisów dotyczących większości amerykańskiej populacji. Centra informacyjne korzystają też z usług innych komercyjnych dostawców baz danych, na przykład firmy Lexis-Nexis.

Z powodu tajności i zakresu zbieranych danych o mieszkańcach centra informacyjne budzą kontrowersje. Organizacje walczące o prawa obywatelskie, na przykład ACLU (American Civil Liberties Union), krytykują gorliwość w zbieraniu informacji o mieszkańcach i brak nadzoru. W centrach informacyjnych pracują zarówno przedstawiciele organów ścigania, jak i personel cywilny. Część osób kwestionuje rolę lokalnych organów ścigania w monitorowaniu podejrzanej aktywności. Na przykład w 2008 roku Duane Kerzic został aresztowany przez służbę ochrony kolei, Amtrak Police, na stacji Penn w Nowym Jorku po tym, jak fotografował pociąg z peronu. Kerzic został skuty kajdankami i umieszczony w areszcie. Okazało się, że chciał jedynie wygrać doroczny konkurs fotograficzny zorganizowany właśnie przez Amtrak.

Choć centra informacyjne mają służyć głównie przeciwdziałaniu terroryzmowi, odgrywają istotną rolę w niektórych śledztwach wymagających zastosowania informatyki śledczej. Te centra jednoznacznie określają, jakiego rodzaju dane cyfrowe są zbierane i przechowywane.

Pierwsza dekada XXI wieku — kryptowaluty, IoT, szyfrowanie i efekt Edwarda Snowdena

W maju 2010 roku Laszlo Hanyecz kupił w Jacksonville dwie pizze za 10 000 bitcoinów (BTC). Wówczas bitcoin był wart mniej niż cent. Dziesięć lat później 10 000 BTC jest wartych ponad 77 milionów dolarów. Choć wielu posiadaczy kryptowalut z pewnością zarabia na życie ciężką pracą, kryptowaluty bez wątpienia ułatwiły dokonywanie płatności między przestępcami. Najbardziej znane są przypadki wykorzystania kryptowalut w sklepach w dark webie, między innymi w serwisach The Silk Road, AlphaBay, HonestCocaine i innych, gdzie walutą używaną do dokonywania nielegalnych zakupów jest bitcoin lub ethereum (ponieważ zapewniają one anonimowość). Prowadzony przez Rossa Ulbrichta serwis The Silk Road był sklepem w dark webie dostępnym wyłącznie za pomocą przeglądarki Tor. Jak na ironię nawet po skutecznym zamknięciu tego serwisu jego sukces w obsłudze anonimowych transakcji narkotykowych spowodował pojawienie się w dark webie innych sklepów prowadzonych przez przestępców. W ostatnich latach wielu twórców, administratorów i sprzedawców powiązanych z takimi sklepami zostało skazanych. Mimo to tego rodzaju serwisy zapewne nadal będą dobrze prosperować. Kryptowaluty są wybierane przez handlarzy narkotykami, ponieważ eliminują konieczność przemytu gotówki przez granice i zmniejszają ilość śladów pozostawianych w wyniku transakcji za pośrednictwem tradycyjnych instytucji finansowych.

Wcześniej wspomniałem, że w latach 2000. błyskawicznie rosła powszechność urządzeń IoT i urządzeń smart home, wykorzystujących sztuczną inteligencję. Urządzenia z wbudowaną sztuczną inteligencją (na przykład z asystentem Alexa) lub systemy monitoringu wizyjnego (na przykład Ring) mogą być ważnym źródłem dowodów elektronicznych.

Lata 2000 są też okresem, w którym szyfrowanie stało się normą, a nie tylko wyborem klientów. Obecnie szyfrowanie całych dysków jest stosowane prawie domyślnie. Najlepiej jest to widoczne wśród producentów smartfonów (zarówno z systemem Android, jak iPhone'ów). Ponadto usprawnienia w obszarze uwierzytelniania dwuskładnikowego sprawiły, że ten protokół zabezpieczeń stał się bardziej popularny w firmach takich jak Apple i Microsoft. Coraz więcej organizacji wymaga dodatkowego uwierzytelniania z użyciem e-maili lub SMS-ów, gdy użytkownik rejestruje nowe urządzenia albo aplikacja jest uruchamiana za pomocą nieznanego urządzenia lub w nowym miejscu. Postępy w dziedzinach szyfrowania i uwierzytelniania stanowią poważne utrudnienie dla informatyków śledczych.

W maju 2013 roku Edward Snowden nagle odszedł z amerykańskiej Agencji Bezpieczeństwa Narodowego (National Security Agency — NSA), zabierając ze sobą wiele tajnych plików. Stał się demaskatorem i ujawnił informacje o tym, jak duże firmy technologiczne przekazują na potrzeby inwigilacji olbrzymie ilości danych agencjom NSA, GCHQ (Government Communications Headquarters) i, ogólniej, grupie Five Eyes. **Five Eyes** jest efektem współpracy agencji wywiadowczych z USA, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii. Niezależnie od tego, czy popierasz postępowanie Edwarda Snowdena, utrudnił on organom ścigania zbieranie danych z niezależnych serwisów, nawet jeśli śledczy uzyskali wezwanie sądowe lub nakaz przeszukania. Niektóre firmy, na przykład Twitter, informują klientów o dochodzeniu, chyba że sąd postanowił inaczej. Można odnieść wrażenie, że inne firmy przyspieszyły prace nad szyfrowaniem oprogramowania i sprzętu, aby chronić prywatność klientów przed inwigilacją ze strony rządu, a nie tylko w celu zwiększenia bezpieczeństwa.

Szkolenia i edukacja

Informatykiem śledczym można zostać na kilka sposobów. Pośrednią drogą dla wielu osób jest praca w organach ścigania. Liczni eksperci zaczynali swoją karierę jako policjanci, a później zostawali skutecznymi śledczymi. Jeśli mieli zdolności informatyczne, a przy tym wydział potrzebował ludzi do spraw wymagających analizy dowodów elektronicznych, mieli okazję stać się specjalistami od informatyki śledczej. Formalne szkolenia w zakresie informatyki śledczej to wciąż stosunkowo nowe zjawisko.

Szkolenia w organach ścigania

Wcześniej wspomniałem, że laboratoria RCFL pomagają organom ścigania współdzielić zasoby, współpracować w sprawach karnych i rozwijać umiejętności w zakresie informatyki śledczej. Prowadzą też formalne szkolenia dla egzaminatorów z RCFL i z jednostek FBI CART. Szkolenia dotyczą zbierania i przechowywania dowodów, a także systemów operacyjnych i używanych w nich systemów plików.

Jednostka CERT (Computer Emergency Response Team) z Carnegie Mellon opracowała szereg narzędzi z zakresu informatyki śledczej przeznaczonych wyłącznie dla organów ścigania. Szkolenia ze stosowania tych narzędzi są dostępne w środowisku FedVTE (Federal Virtual Training Environment) jednostki CERT.

FLETC (Federal Law Enforcement Training Center) to międzyagencyjna organizacja z siedzibą w Glynco w stanie Georgia zajmująca się szkoleniem organów ścigania. Współpracuje z nią ponad 80 agencji federalnych z całego kraju. Jeden z oferowanych programów, SCERS, jest przeznaczony dla specjalistów od odzyskiwania danych z zajętych komputerów. FLETC prowadzi też szkolenia z zagadnień takich jak analiza śledcza komputerów z systemem macOS i analiza śledcza sieci.

NW3C (National White Collar Crime Center) jest agencją, która prowadzi szkolenia i konsultacje dla organów ścigania i jednostek odpowiedzialnych za zapewnienie przestrzegania prawa. NW3C oferuje kursy z różnych dziedzin informatyki śledczej, w tym z analizy śledczej telefonów komórkowych, wykorzystania internetu w dochodzeniach, systemów operacyjnych, systemów plików oraz zbierania i analizy dowodów elektronicznych. Jednym ze znanych kursów tej agencji jest STOP (SecureTechniques for Onsite Preview). Jest on przeznaczony dla kuratorów sądowych, detektywów i policjantów, którzy przeprowadzają przeszukania lub domowe wizyty kontrolne oraz muszą szybko sprawdzać komputery w sposób zgodny z przepisami prawa i zasadami zawodowymi. Na przykład kurator sądowy może szukać zdjęć na komputerze osoby skazanej za przestępstwa na tle seksualnym.

INTERPOL zapewnia organom ścigania z całego świata pomoc w zakresie informatyki śledczej. W kwietniu 2009 roku Uniwersytet Dubliński i INTERPOL uruchomiły program szkoleń z zakresu dochodzeń w przestępstwach elektronicznych. Program polega nie tylko na prowadzeniu kursów, ale też ma ułatwiać wymianę akademicką w dziedzinie informatyki śledczej w celu rozwijania umiejętności specjalistów z tego obszaru. Uczelnia oferuje prestiżowe studia magisterskie z dziedziny informatyki śledczej i cyberprzestępczości, dostępne wyłącznie dla przedstawicieli organów ścigania z całego świata.

Inną organizacją nastawioną na wymianę pomysłów i doświadczeń w dziedzinie informatyki śledczej jest **CTIN** (Computer Technology Investigators Network). Jej członkami mogą zostać przedstawiciele organów ścigania, specjaliści od bezpieczeństwa korporacyjnego i akademicy. Z kolei **InfraGard** jest podlegającą FBI publiczno-prywatną agencją promująca wymianę informacji między sektorami prywatnym i publicznym w kwestiach związanych z terroryzmem, wywiadem i bezpieczeństwem. InfraGard ma filie w różnych miejscach, a należeć do niej może każdy obywatel Stanów Zjednoczonych (kandydaci są weryfikowani przez FBI).

Kursy w szkołach średnich

Wiele szkół średnich w Stanach Zjednoczonych wprowadziło zajęcia z informatyki śledczej dla uczniów z profili prawnego i technicznego. Takie kursy prowadzi na przykład Departament Edukacji Nowego Jorku, z którym współpracowałem przez ponad dekadę, tworząc program kursów z informatyki śledczej i cyberbezpieczeństwa dla uczniów szkół średnich. Program informatyki śledczej jest znakomitym sposobem do nauczania zawiłych aspektów dochodzeń z wykorzystaniem dowodów elektronicznych.

Kursy uniwersyteckie

Wiele uniwersytetów prowadzi kursy informatyki śledczej na studiach licencjackich i magisterskich. Najbardziej prestiżowe uczelnie, które oferują studia z informatyki śledczej, to Champlain College, Uniwersytet Purdue i Uniwersytet Carnegie Mellon. Dwie ostatnie współpracują w dziedzinie informatyki śledczej z organami ścigania. Inny znany program informatyki śledczej jest prowadzony przez Uniwersytet w Bloomsburgu. Kierunek informatyki śledczej jest też oferowany przez inne uczelnie, na przykład Uniwersytet Pace, który także ściśle współpracuje z organami ścigania.

Certyfikaty zawodowe

Uzyskanie dyplomu z informatyki śledczej, informatyki, a nawet systemów informatycznych może zapewnić solidne podstawy w omawianej dziedzinie. Dyplom poparty certyfikatami oznacza wyższe kompetencje i powoduje, że kandydatowi jeszcze łatwiej jest przekonać do siebie potencjalnego pracodawcę. Dzieje się tak, ponieważ wiele kursów certyfikacyjnych jest prowadzonych przez specjalistów i obejmuje praktyczne szkolenia z użyciem profesjonalnych narzędzi.

W następnych podpunktach opisałem certyfikaty z dziedziny informatyki śledczej, które uwiarygodniają kwalifikacje informatyka śledczego. Lista ta nie jest jednak kompletna.

Ogólnodostępne certyfikaty zawodowe

IACIS (International Association of Computer Investigative Specialists) to organizacja non profit, której misją jest edukowanie organów ścigania w dziedzinie informatyki śledczej. Jednym z najbardziej znanych certyfikatów w branży jest CFCE (Certified Forensic Computer Examiner) przyznawany właśnie przez IACIS.

John Mellon był aktywnym członkiem IACIS, zanim założył organizację ISFCE (International Society of Forensic Computer Examiners). Opracował certyfikat CCE (Certified Computer Examiner) przyznany po raz pierwszy w 2003 roku. ISFCE ma cztery ośrodki testowe i przeprowadza testy kompetencji dla ASCLD/LAB (American Society of Crime Laboratories Directors/Laboratory Accreditation Board). Testy te pozwalają uzyskać najbardziej cenione certyfikaty dla laboratoriów śledczych. ASCLD jest zawodowym stowarzyszeniem non profit skupiającym dyrektorów i kierowników laboratoriów kryminalistyki, którzy chcą promować doskonałość w dziedzinie nauk śledczych, w tym informatyki śledczej. Akredytacje ASCLD/LAB mają laboratoria informatyki śledczej USSS i wielu innych organów ścigania, co dowodzi znaczenia tych certyfikatów.

Ogólnie dostępne są liczne inne certyfikaty niezależne od producentów oprogramowania lub sprzętu. Na przykład IACRB (Information Assurance Certification Review Board) przyznaje certyfikat CCFE (Certified Computer Forensics Examiner). Aby go uzyskać, kandydat musi udowodnić swoją wiedzę w następujących obszarach:

- kwestie etyczne i prawne,
- proces śledczy;

- narzędzia informatyki śledczej;
- odzyskiwanie i integralność dowodów z dysków twardych;
- odzyskiwanie i integralność dowodów elektronicznych;
- analiza śledcza systemów plików;
- analiza i łączenie dowodów;
- odzyskiwanie dowodów z systemu Windows;
- analiza śledcza sieci i pamięci nietrwałej;
- pisanie raportów.

Certyfikat CFC (Certified Forensic Consultant) przyznawany przez ACFEI (American College of Forensics Examiners International) dotyczy prawnych aspektów informatyki śledczej w Stanach Zjednoczonych. Program certyfikacyjny pozwala zdobyć wiedzę w następujących obszarach:

- postępowania sądowe;
- federalne przepisydotyczące dowodów;
- proces zbierania dowodów;
- sporządzanie notatek;
- wizja lokalna;
- raport pisemny;
- umowy o świadczenie usług doradztwa prawnego;
- kategorie świadków;
- opinia biegłego sądowego;
- przygotowania do zeznań;
- czego można oczekiwać w trakcie składania zeznań;
- przygotowania do procesu;
- zeznawanie w trakcie procesu;
- co zabrać do sądu;
- branża konsultacji prawnych.

ACFEI prowadzi też szkolenia i testy na potrzeby certyfikatu CrFA dla audytorów śledczych (Certified Forensic Accountant). **Audytor śledczy** ma wiedzę z zakresu rachunkowości i uczestniczy w dochodzeniach finansowych.

Instytut SANS (SysAdmin, Audit, Network, Security) od czasu jego utworzenia w 1989 roku prowadzi szkolenia dla specjalistów od bezpieczeństwa w sektorach publicznym i prywatnym. SANS ma w ofercie także szkolenia z informatyki śledczej i prowadzi kurs z zakresu reagowania na incydenty i dochodzeń z wykorzystaniem informatyki śledczej. Kurs zapewnia wiedzę potrzebną do uzyskania certyfikatu GCFA (GIAC Certified Forensic Analyst). Założona w 1999 roku organizacja GIAC (Global Information Assurance Certification) ocenia umiejętności specjalistów z branży zabezpieczeń komputerowych.

Certyfikaty zawodowe dla specjalistów od zabezpieczeń

Choć bezpieczeństwo teleinformatyczne i informatyka śledcza to dwie różne dziedziny, wzajemnie się uzupełniają. Dlatego wielu informatyków śledczych posiada certyfikaty z obszaru bezpieczeństwa teleinformatycznego. W obsłudze incydentów związanych z bezpieczeństwem (takich jak włamania do sieci) uczestniczyć mogą zarówno specjaliści od bezpieczeństwa, jak i eksperci od informatyki śledczej. Specjalista od bezpieczeństwa może zapewniać informacje na temat kategorii naruszenia zabezpieczeń i zakresu ataku, natomiast informatyk śledczy często może ustalić dowodowy pozostawione przez napastnika.

Program CSIH (Certified Security Incident Handler) to doskonały kurs dla informatyków śledczych. Jest prowadzony przez CERT (Computer Emergency Response Team), jednostkę będącą częścią instytutu SEI (Software Engineering Institute) na Uniwersytecie Carnegie Mellon. SEI to finansowane na poziomie federalnym centrum badań i rozwoju utrzymywane przez Departament Obrony Stanów Zjednoczonych. CERT prowadzi szkolenia dla administratorów sieci i innych pracowników wsparcia technicznego. Dotyczą one między innymi identyfikowania istniejących i potencjalnych zagrożeń sieci. Prowadzi też kursy z zakresu radzenia sobie ze złamaniem zabezpieczeń. Zespół kryminalistyczny CERT-u ściśle współpracuje z organami ścigania przy projektach badawczych dotyczących rozwiązań, których brakuje w komercyjnych narzędziach dla informatyków śledczych.

Informatycy śledczy, przede wszystkim z sektora prywatnego, dość często posiadają certyfikat CISSP (Certified Information Systems Security Professional). Jest on oferowany przez grupę ISC^2 (International Information Systems Security Certification Consortium). Certyfikat CISSP został formalnie zatwierdzony przez Departament Obrony w zakresie wiedzy technicznej i menedżerskiej. Ten istotny certyfikat można uzyskać po zdaniu egzaminu z zakresu Common Body of Knowledge (CBK), gdzie uwzględniane są następujące obszary bezpieczeństwa:

- kontrola dostępu;
- bezpieczeństwo procesu tworzenia aplikacji;
- zapewnienie ciągłości działania firmy i planowanie przywracania stanu po katastrofach;
- kryptografia;
- zarządzanie bezpieczeństwem informacji i ryzykiem;
- kwestie prawne, regulacje, dochodzenia i zgodność z zasadami;
- bezpieczeństwo operacji;
- zabezpieczenia fizyczne;
- architektura i projektowanie zabezpieczeń;
- zabezpieczenia telekomunikacyjne i sieciowe.

Aby zdać egzamin CISSP, trzeba uzyskać wynik przynajmniej 700 punktów na 1000 na podstawie 250 pytań wielokrotnego wyboru. Osoba podchodząca do egzaminu CISSP musi wykazać co najmniej pięcioletnie doświadczenie w minimum dwóch z dziesięciu dziedzin. Sprawdzane jest też, czy kandydat nie ma przeszłości kryminalnej. Konieczne jest także przestrzeganie

kodeksu etycznego CISSP. Po otrzymaniu certyfikatu trzeba uzyskać punkty za ustawiczne kształcenie (Continuing Professional Credits — CPE), aby go utrzymać.

Innym ważnym certyfikatem z dziedziny zabezpieczeń często posiadanym przez informatyków śledczych jest CISM (Certified Information Security Manager). Podobnie jak CISSP, jest przyznawany specjalistom od bezpieczeństwa. Różni się od certyfikatu CISSP, ponieważ otrzymują go menedżerowie ds. bezpieczeństwa informacji mający doświadczenie w następujących dziedzinach:

- zarządzanie bezpieczeństwem informacji;
- zarządzanie ryzykiem związanym z informacjami;
- rozwój programów z zakresu bezpieczeństwa informacji;
- zarządzanie programami zakresu bezpieczeństwa informacji;
- reagowanie na incydenty i radzenie sobie z nimi.

Wymogiem dla posiadaczy certyfikatów CISM (podobnie jak dla osób z certyfikatem CISSP) jest ustawiczne kształcenie się i zdobywanie najnowszej wiedzy z obszaru zarządzania bezpieczeństwem informacji.

Certyfikaty zawodowe przyznawane przez producentów oprogramowania z dziedziny informatyki śledczej

Większość producentów oprogramowania z dziedziny informatyki śledczej oferuje kursy certyfikacyjne. Znani producenci oprogramowania do tworzenia obrazów to Cellebrite/BlackBag, AccessData, opentext i X-Ways Forensics.

- BlackBag Technologies oferuje różnorodne bootcampy z zakresu analizy śledczej systemów macOS i Windows. Jednym z popularnych certyfikatów tej firmy jest BCE (BlackLightCertifiedExaminer).
- AccessData oferuje kursy AccessDataBootcamp i zajęcia z analizy śledczej systemów Windows imacOS, materiałów internetowych oraz urządzeń mobilnych. Najbardziej znanym certyfikatem tej firmy jest ACE (AccessDataCertifiedExaminer). Egzamin sprawdza umiejętności użytkownika w korzystaniu z narzędzi FTK Imager, Registry Viewer i PRTK.
- Opentext także prowadzi szkolenia i egzaminy dla informatyków śledczych. Osoba, która potrafi udowodnić biegłość w korzystaniu z narzędzia EnCase, otrzymuje certyfikat EnCE (EnCaseCertifiedExaminer).
- X-WaysForensics prowadzi regularne szkolenia i egzaminy ze znajomości narzędzia X-WaysForensics (służącego do wykonywania obrazów bitowych) i produktu WinHex. Wykładowcy z X-Ways prowadzą zwykle pięciodniowe kursy. Pierwsze dwa dni są poświęcone systemom plików, a pozostałe — narzędziom śledczym.

Certyfikaty BCE, ACE i EnCE, a także szkolenia firmy X-Ways Forensics są dostępne dla specjalistów z sektorów prywatnego i publicznego.

Podsumowanie

Informatyka śledcza (inaczej kryminalistyka cyfrowa) wykorzystuje dane cyfrowe do rozwiązywania spraw kryminalnych. Jest to dziedzina naukowa, która — podobnie jak wszystkie obszary analiz śledczych — wymaga ścisłego stosowania się do przepisów prawnych. Informatyka śledcza jest stosowana w wielu różnego rodzaju dochodzeniach w sprawach karnych, ale można się nią posługiwać także w sprawach cywilnych lub w ramach reagowania na włamania do sieci. Informatyk śledczy korzysta z różnych urządzeń i aplikacji do pobierania i analizowania plików. Stosowane są na przykład narzędzia do tworzenia obrazów bitowych, które generują bit po bicie kopię zawartości urządzenia osoby podejrzanej. Samo znalezienie dowodu nie zawsze wystarcza. Ważne jest też, aby wykazać kontrolę, własność i zamiary podejrzanego. Dowodami elektronicznymi mogą być na przykład e-maile, zdjęcia, filmy, odwiedziny witryn i wyrażenia wyszukiwane w internecie.

Skuteczny informatyk śledczy powinien posiadać umiejętności z różnych obszarów, w tym z informatyki, prawa materialnego i procesowego, kryminologii, matematyki, komunikacji i lingwistyki. Te umiejętności można zdobyć w różny sposób, na przykład w trakcie szkoleń zawodowych (co jest powszechne w organach ścigania), w czasie studiów lub na kursach certyfikacyjnych. Osoby zainteresowane karierą w dziedzinie informatyki śledczej mają do wyboru wiele stanowisk w sektorach prywatnym i publicznym.

Pojawienie się komputerów osobistych w latach 80. ubiegłego wieku spowodowało, że użytkownicy częściej korzystają z tych urządzeń w domach. Wraz z tym wzrosła liczba przestępstw związanych z komputerami. W efekcie agencje rządowe zaczęły przeznaczać środki na informatykę śledczą, czego dowodem jest utworzenie jednostki CART (Computer Analysis and Response Team) w FBI. Wprowadzenie w latach 90. przeglądarek internetowych sprawiło, że użytkownicy komputerów osobistych zaczęli korzystać z internetu. Ostatecznie internet stał się miejscem do zdobywania cennych informacji na temat podejrzanych, a także źródłem obciążających dowodów. Informatyką śledczą posługują się liczne agencje w ramach Departamentu Bezpieczeństwa Wewnętrznego. Ponadto INTERPOL znacznie rozbudował swoje zasoby w obszarze informatyki śledczej w reakcji na rozwój korzystających z internetu międzynarodowych siatek przestępczych. Już teraz potrzebna jest współpraca między Departamentem Bezpieczeństwa Wewnętrznego i innymi państwami, jednak w przyszłości będzie ona jeszcze ważniejsza, zwłaszcza w obszarze informatyki śledczej.

W tabeli 1.1 przedstawiłem chronologię wydarzeń z dziedziny informatyki śledczej i ważnych osiągnięć technologicznych, które wpłynęły na ten obszar.

TABELA 1.1. Historia informatyki śledczej i ważnych wydarzeń w świecie informatyki

Rok	Wydarzenie
1981	Wprowadzenie komputera 5150 PC przez IBM
1984	Utworzenie przez FBI programu Magnetic Media Program (znanego później jako CART)
1984	Założenieorganizacji NCMEC (National Center for Missing and Exploited Children)
1986	Utworzenie jednostki ECTF (ElectronicCrimesTask Force) przez USSS
1986	Uchwalenie ustawy o oszustwach i nadużyciach komputerowych przez Kongres Stanów Zjednoczonych
1993	Pierwsza międzynarodowa konferencja poświęcona dowodom komputerowym
1994	Uchwalenie przez Kongres ustawy o przestępczości; rozpoczęcie przez USSS pracy nad zwalczaniem przestępstw przeciwko dzieciom
1994	Udostępnienie Mosaic Netscape — pierwszej graficznej przeglądarki internetowej
1995	Założenieorganizacji IOCE (International Organization on Computer Evidence)
1996	ZałożenieprzezUSSS jednostki ECTF (New York Electronic Crimes Task Force)
1998	Powstanie Europolu
1999	Utworzenie pierwszego laboratorium RCFL w San Diego
2000	Rozpoczęcie stosowania narzędzia ILook przez IRS-CID
2001	Uchwalenie ustawy USA PATRIOT, która nakazuje USSS utworzenie jednostek ECTF w całym kraju
2001	Opracowanie przez INTERPOL bazy danych dotyczącej wykorzystywanych dzieci (ICAID)
2002	Utworzenie Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych
2003	Uchwalenie ustawy PROTECT w celu przeciwdziałania wykorzystywaniu dzieci
2003	Powstanie centrów informacyjnych
2003	Utworzenie przez Europol centrum EC3 (EuropeanCybercrime Center)
2004	Powstanie serwisu Facebook
2007	Utworzenie instytutu NCFI
2008	Zatwierdzenie powstania jednostki ComputerForensics Analysis Unit INTERPOL-u
2009	Utworzenie pierwszej europejskiej jednostki ECTF (we Włoszech)
2009	Rozpoczęcie rejestrowania transakcji w księdze głównej bitcoina
2010	Utworzenie drugiej europejskiej jednostki ECTF (w Wielkiej Brytanii)
2011	Uchwalenie ustawy PATRIOT Sunsets Extension
2013	Ucieczka Edwarda Snowdena do Rosji po ujawnieniu poufnych danych z NSA
2015	Zakończenie procesu w sprawie serwisu The Silk Road skazaniem założyciela, Rossa Ulbrichta
2015	Uchwalenie ustawy o wymianie informacji z zakresu cyberbezpieczeństwa (Cybersecurity Information Sharing)
2016	Uchwalenie ustawy o uprawnieniach śledczych w Wielkiej Brytanii
2017	Wprowadzenie systemu plików APFS przez Apple w systemie iOS 10.3
2018	Wprowadzenie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)

Najważniejsze pojęcia

Algorytm — zestaw kroków stosowanych w celu rozwiązania problemu.

BitLocker — narzędzie szyfrujące wprowadzone w wersjach Ultimate i Enterprise systemu Microsoft Windows Vista. Umożliwia szyfrowanie na poziomie plików, katalogów i dysków.

Narzędzie do tworzenia obrazów bitowych — narzędzie, które tworzy bit po bicie kopię pierwotnego nośnika, w tym plików oznaczonych do usunięcia.

Łańcuch dowodowy — dokumentacja obejmująca każdą osobę, która miała kontakt z dowodem od momentu jego pozyskania, przez analizy, po przedstawienie sądowi.

Komputer kliencki — komputer, który żąda zasobu z serwera.

Monitoring wizyjny — obserwowanie obrazu transmitowanego w określone miejsce.

CART (Computer Analysis and Response Team) — jednostka FBI odpowiedzialna za wspomaganie dochodzeń wymagających analiz z obszaru informatyki śledczej.

Bezpieczeństwo teleinformatyczne — dziedzina zapobiegania nieuprawnionemu dostępowi do komputerów i powiązanych z nimi zasobów.

CTIN (Computer Technology Investigators Network) — organizacja zajmująca się wymianą idei i doświadczeń z dziedziny informatyki śledczej.

Informatyka śledcza — dziedzina zajmująca się zbieraniem, analizowaniem i wykorzystywaniem dowodów elektronicznych w sprawach cywilnych i karnych.

eDiscovery — proces odzyskiwania danych cyfrowych.

ECTF (Electronic Crimes Task Force) — ogólnokrajowa sieć zajmująca się zwalczaniem cyberprzestępstw.

Szyfrowanie — proces przekształcania zwykłego tekstu na nieczytelny format z użyciem wzoru matematycznego.

Dowód uniewinniający — dowód pozwalający dowieść niewinności oskarżonego.

FLETC (Federal Law Enforcement Training Center) — międzyagencyjna organizacja szkoląca organy ścigania. Współpracuje z ponad 80 federalnymi agencjami z całego kraju.

Metadane pliku — informacje o pliku. Mogą obejmować datę jego utworzenia, modyfikacji i ostatniego dostępu, a także dane użytkownika, który utworzył plik.

Five Eyes — wspólny program agencji wywiadowczych z USA, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii.

Audytor śledczy — osoba z wiedzą z obszaru księgowości uczestnicząca w dochodzeniach w sprawach finansowych.

GPS (ang. *Global Positioning System*) — system wykorzystywany w urządzeniach, które odbierają dane z satelitów w celu ustalenia lokalizacji geograficznej.

Dowód obciążający — dowód często prowadzący do skazania przestępcy.

InfraGard — publiczno-prywatna agencja w FBI, która zachęca do wymiany między sektorami prywatnym i publicznym informacji na tematy związane z terroryzmem, wywiadem i zabezpieczeniami.

INTERPOL — największa na świecie międzynarodowa organizacja policyjna. Skupia 188 państw członkowskich.

NCMEC (National Center for Missing and Exploited Children) — agencja, której zadaniem jest pomoc w znajdowaniu zaginionych dzieci i zwalczaniu (seksualnego) wykorzystywania nieletnich.

NW3C (National White Collar Crime Center) — agencja zapewniająca szkolenia i wsparcie dochodzeniowe organom ścigania i wymiaru sprawiedliwości.

Pamięć RAM (ang. *Random Access Memory*) — często nazywana też pamięcią nietrwałą, ponieważ po wyłączeniu komputera jej zawartość zwykle znika. Aktualne działania i procesy użytkownika, w tym aktywność w internecie, są zapisywane w pamięci RAM.

RCFL (Regional Computer Forensics Laboratory) — finansowane przez FBI laboratorium, które szkoli organy ścigania z zakresu korzystania z narzędzi informatyki śledczej i umożliwia współpracę przy dochodzeniach w sprawach karnych.

Skimmer — urządzenie używane do sczytywania informacji zapisanych na pasku magnetycznym karty bankomatowej, kredytowej lub debetowej.

Manipulowanie dowodami — ukrywanie, uszkadzanie, modyfikowanie lub fałszowanie dowodów powiązanych ze śledztwem.

Serwer WWW — udostępnia dokumenty HTML i powiązane zasoby w odpowiedzi na żądania od komputera klienckiego.

Sprawdzian wiedzy

TEMATY DO DYSKUSJI NA ZAJĘCIACH

1. W jaki sposób można zostać informatykiem śledczym?
2. Czym jest informatyka śledcza i jak korzysta się z niej w trakcie dochodzeń?
3. Jakiego rodzaju działalność przestępcza jest prowadzona w sklepach w dark webie i dlaczego odbywa się z takim powodzeniem?

PYTANIA WIELOKROTNEGO WYBORU

1. Które z poniższych stwierdzeń najlepiej definiuje informatykę śledczą?
   - **A.** Informatyka śledcza polega na wykorzystywaniu dowodów do wykrywania sprawców przestępstw komputerowych
   - **B.** Informatyka śledcza polega na wykorzystywaniu dowodów elektronicznych do wykrywania sprawców przestępstw
   - **C.** Informatyka śledcza służy wyłącznie do odzyskiwania usuniętych plików z komputerów
   - **D.** Informatyka śledcza służy wyłącznie do badania komputerów stacjonarnych i laptopów
2. Czego dokumentacją jest łańcuch dowodowy?
   - **A.** Policjantów, którzy zatrzymali podejrzanego
   - **B.** Listów i e-maili wymienianych w trakcie dochodzenia
   - **C.** Osób, które miały kontakt z dowodem w danej sprawie
   - **D.** Żadne z powyższych
3. Które z poniższych przedmiotów mogą mieć wartość dowodową dla informatyków śledczych?
   - **A.** Karta SIM
   - **B.** Xbox
   - **C.** Cyfrowy aparat fotograficzny
   - **D.** Wszystkie powyższe
4. Które z poniższych stwierdzeń najlepiej opisuje narzędzie do tworzenia obrazów bitowych?
   - **A.** Tworzy bit po bicie kopię pierwotnego nośnika
   - **B.** Często zapewnia śledczemu dostęp do usuniętych plików
   - **C.** Ani a, ani b
   - **D.** Zarówno a, jak i b
5. Które z poniższych stwierdzeń opisują zalety dowodów w postaci e-maili?
   - **A.** Zwykle są dostępne w kilku miejscach
   - **B.** Często łatwiej je znaleźć niż inne rodzaje dowodów
   - **C.** Są dopuszczalne w wielu sprawach
   - **D.** Wszystkie powyższe
6. Które z poniższych stwierdzeń dotyczących zdjęć nie są prawdziwe?
   - **A.** Zdjęcia mogą być dowodem na to, gdzie znajdował się podejrzany
   - **B.** Zdjęć nie można łatwo znaleźć za pomocą narzędzi do tworzenia obrazów bitowych (takich jak FTK)

C. Zdjęcie może pozwolić w ustaleniu producenta i modelu aparatu cyfrowego

D. Obecnie stosowany jest jeden rodzaj zdjęć cyfrowych

7. Które z poniższych określeń najlepiej opisuje ukrywanie, modyfikowanie i uszkadzanie dowodów?
   A. Niszczenie dowodów
   B. Manipulowanie dowodami
   C. Dowody obciążające
   D. Dowody uniewinniające
8. W ramach której agencji rządowej działa jednostka CART?
   A. USSS
   B. FBI
   C. CIA
   D. ICE
9. Która z poniższych ustaw powołała Departament Bezpieczeństwa Wewnętrznego i nakazała USSS utworzenie w całym kraju jednostek ECTF?
   A. Health Insurance Portability and Accountability
   B. Children's Online Privacy Protection
   C. PROTECT
   D. USA PATRIOT
10. Które z poniższych stwierdzeń dotyczących laboratoriów RCFL nie są prawdziwe?
    A. Z laboratoriów RCFL mogą korzystać obrońcy w sprawach karnych
    B. Założenie laboratoriów RCFL było finansowane przez FBI
    C. Laboratoria RCFL są wykorzystywane nie tylko w dochodzeniach, ale też prowadzą szkolenia z zakresu informatyki śledczej
    D. Laboratoria RCFL istnieją w Stanach Zjednoczonych i Europie

UZUPEŁNIJ ZDANIA

1. _____ to zestaw kroków potrzebnych do rozwiązania problemu.
2. Informatyka _____ wykorzystuje dowody elektroniczne w dochodzeniach mających na celu wykrycie sprawców przestępstw.
3. Bezpieczeństwo _____ to dziedzina obejmująca zapobieganie nieuprawnionemu dostępowi do komputerów i powiązanych z nimi zasobów.
4. Oskarżony może dowieść swojej niewinności dzięki dowodom _____.
5. Proces przekształcania zwykłego tekstu na nieczytelny format na podstawie wzoru matematycznego jest nazywany _____.
6. Największa na świecie międzynarodowa organizacja policyjna to _____.

7. Krótkotrwała ulotna pamięć, której zawartość znika po wyłączeniu komputera, jest nazywana pamięcią _____.
8. _____ to urządzenie używane do sczytywania informacji zapisanych na pasku magnetycznym karty bankomatowej, kredytowej lub debetowej.
9. Serwer _____ udostępnia dokumenty HTML i powiązane zasoby w odpowiedzi na żądania od komputera klienckiego.
10. _____ jest publiczno-prywatną agencją FBI, która promuje wymianę między sektorami prywatnym i publicznym informacji z zakresu terroryzmu, wywiadu i bezpieczeństwa.

PROJEKTY

Przeprowadź dochodzenie

Jesteś informatykiem śledczym w lokalnych organach ścigania i przydzielono Cię do dochodzenia w pewnej sprawie. Podejrzany, Michał Malewicz, był dyrektorem ds. rozwoju produktu w firmie opracowującej oprogramowanie. Został on wezwany do wyjaśnienia okoliczności wykonania kilki kosztownych rozmów telefonicznych. Analiza rejestru rozmów wykazała, że Malewicz dzwonił do konkurencyjnej chińskiej firmy mającej oddziały w USA. Po skonfrontowaniu go z uzyskanymi rejestrami, Malewicz stwierdził, że musi skonsultować się z prawnikiem i odmówił dalszych wyjaśnień. Następnego dnia nie stawił się w pracy. Kolejnego dnia firma skontaktowała się z lokalnymi organami ścigania. Malewicz został zatrzymany, gdy próbował dostać się na pokład samolotu do Pekinu dwa dni po przesłuchaniu w sprawie kontaktów z konkurencją. Na lotnisku agenci ABW ujawnili torbę wypełnioną płytami CD, trzy dyski twarde SATA i pięć pamięci USB.

Wymień rodzaje dowodów elektronicznych, jakie mogą być przydatne w tym dochodzeniu.

Sprawdź możliwości zatrudnienia dla informatyka śledczego

Opisz, dlaczego w najbliższych latach informatycy śledczy nadal będą potrzebni. W odpowiedzi podaj statystyki dotyczące wzrostu liczby określonych rodzajów przestępstw.

Poszukaj informacji o agencjach federalnych

Opracuj schemat organizacyjny z wszystkimi agencjami federalnymi zajmującymi się informatyką śledczą. Zacznij od Departamentu Bezpieczeństwa Wewnętrznego, a następnie podaj nazwę każdej agencji i tam, gdzie to wskazane, nazwę jednostki odpowiedzialnej za informatykę śledczą.

Silk Road

Przejrzyj doniesienia medialne i materiały sądowe dotyczące procesu w sprawie platformy The Silk Road. Napisz raport na temat wykorzystania przez FBI i DHS dowodów elektronicznych, które ostatecznie doprowadziły do skazania Rossa Ulbrichta.

WYKRYJ. ZNAJDŹ DOWODY. ZABEZPIECZ JE I ZBADAJ!

Nasilanie się zjawiska cyberprzestępczości sprawia, że prowadzenie dochodzeń kryminalnych wymaga specjalnych umiejętności i wiedzy technicznej. Bez odpowiedniego materiału dowodowego niemożliwe jest oskarżenie i osądzenie winnych. Sytuację utrudnia rozwój technologii: serwisy społecznościowe, urządzenia mobilne czy internet rzeczy są wykorzystywane do popełniania przestępstw na wiele dotychczas nieznanych sposobów. W tych warunkach informatycy śledczy są bardzo potrzebni, a specjaliści dysponujący aktualną wiedzą — wręcz bezcenni.

Oto znakomity i w pełni zaktualizowany przewodnik po informatyce śledczej, uwzględniający najnowsze techniki, narzędzia i rozwiązania. W książce omówiono praktyczne aspekty zarówno umiejętności technicznych, jak i spraw ważnych z punktu widzenia prowadzenia dochodzeń w internecie i laboratorium. Opisano istotne zagadnienia dotyczące dokumentacji, dopuszczalności dowodów i innych aspektów prawnych. Szczegółowo zaprezentowano technologie ubieralne, analizy śledcze urządzeń IoT, kwestie komunikacji 5G, analizy śledczej pojazdów i analiz aplikacji mobilnych. Opracowanie uwzględnia też postępy w dziedzinie reagowania na incydenty oraz nowe techniki badania urządzeń mobilnych. Treści zostały uzupełnione praktycznymi zadaniami, realistycznymi przykładami oraz fascynującymi studiami przypadków.

DOWIESZ SIĘ, JAK:

- wygląda praca informatyka śledczego
- wykorzystywać nowinki technologiczne w procesie zbierania dowodów
- rozpoznać naruszenia bezpieczeństwa i prawidłowo reagować na incydenty
- badać oszustwa finansowe
- analizować technologie ubieralne i urządzenia IoT
- sprawić, by zdobyte dowody zostały uznane w sądzie

DR DARREN R. HAYES jest uznanym ekspertem w dziedzinie informatyki śledczej i cyberbezpieczeństwa. Wykłada na Pace University, jest autorem kursów informatyki śledczej dla studentów. Kieruje laboratorium informatyki śledczej. Współpracuje z nowojorską policją, prokuraturą, Departamentem Bezpieczeństwa Krajowego Stanów Zjednoczonych, brytyjską Narodową Agencją ds. Przestępczości i wieloma innymi jednostkami. Ma status biegłego sądowego w amerykańskim sądzie federalnym.

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

INFORMATYKA W NAJLEPSZYM WYDANIU

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-283-7569-7

Cena: 149,00 zł

Pearson