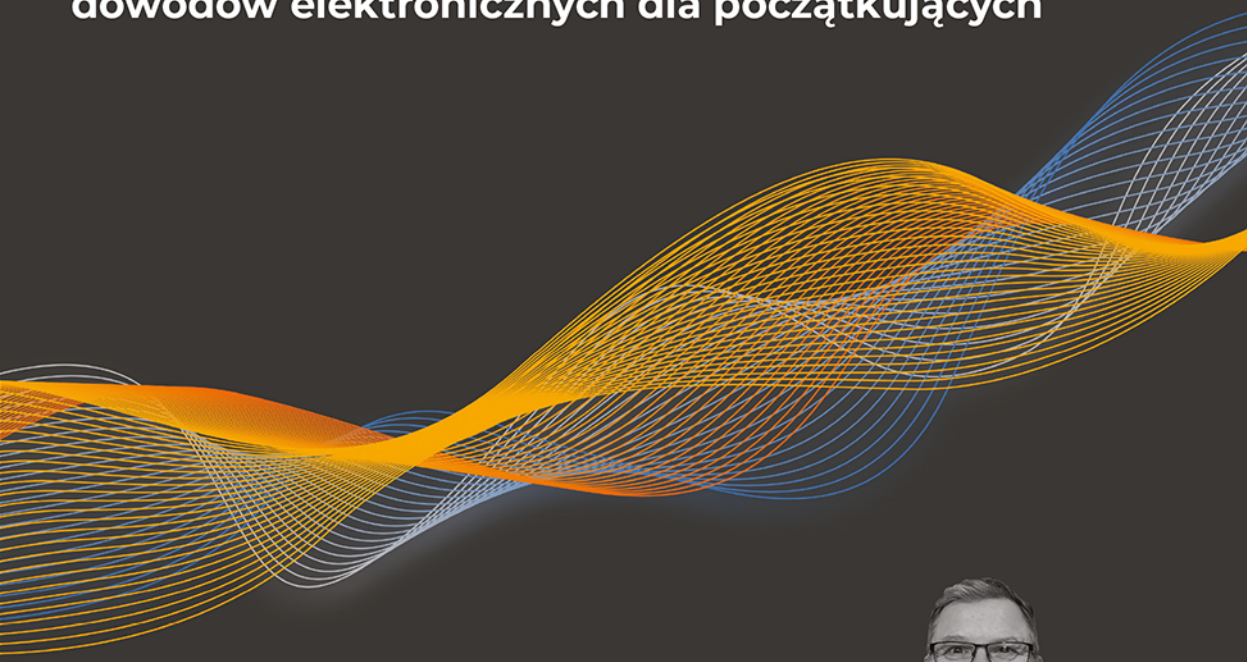
Wydanie II

Informatyka śledcza

Gromadzenie, analiza i zabezpieczanie dowodów elektronicznych dla początkujących



William Oettinger

Helion

packt

Tytuł oryginału: Learn Computer Forensics: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence, 2nd Edition

Tłumaczenie: Filip Kamiński

ISBN: 978-83-289-0171-1

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/inslg2
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

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

Printed in Poland.

Spis treści

Rozdział 10

Śledztwa w sieci

Jakie informacje można znaleźć w internecie? Czy da się w nim zidentyfikować potencjalnego podejrzanego? Czy istnieją bazy danych, w których możemy znaleźć informacje na temat podejrzanych? Czy przy użyciu zasobów internetowych można przeprowadzić prowokację? Są to ważne pytania, a odpowiedź na większość z nich jest twierdząca. Gdy poprosisz kogoś o znalezienie informacji o jakiejś osobie, jednym z pierwszych miejsc, w których osoba ta przeprowadzi wyszukiwanie, będzie Google. Wyszukiwarka ta zwraca wiele informacji, które mogą, ale nie muszą, dotyczyć osoby będącej przedmiotem wyszukiwania. Google da Ci odnośniki do wielu różnych zasobów, które warto przeanalizować, ale zwróci również linki do zakamarków sieci, w których nie znajdziesz żadnych pomocnych informacji.

Kiedy czytasz te słowa, organy ścigania i organizacje prywatne prowadzą śledztwa w sieci. Organy ścigania poszukują śladów działalności przestępczej np. dorosłych chcących wykorzystać seksualnie dzieci. Firmy weryfikują potencjalnych nowych pracowników i zbierają informacje na temat konkurencji, a uczelnie wyższe starają się przewidzieć liczbę studentów w kolejnych latach. Z pewnością słyszałeś kiedyś o zwolnieniu z pracy (lub usunięciu studenta z college'u) z powodu znalezienia w sieci wpisów, w których dana osoba zamieszczała niepochlebne informacje na temat pracodawcy (uczelni) lub inne oburzające treści.

W tym rozdziale omówię następujące zagadnienia:

- śledztwa pod przykrywką,
- wyszukiwanie informacji o podejrzanym,
- rejestrację czynności wykonywanych w toku śledztwa w sieci.

Śledztwa pod przykrywką

Jak prowadzi się śledztwo w sieci? Czy w sieci poszukuje się zasobów, czy bada aktywność użytkownika w cyfrowym świecie? Prowadzenie śledztwa w sieci polega na systematycznym przeszukiwaniu internetu w celu identyfikacji, zachowania, analizy

i zaraportowania informacji na temat przedmiotu dochodzenia. Większość z nas zna przypadki, w których ktoś został zwolniony za coś, co opublikował w sieci. Może był to niezbyt przemyślany tweet, film na TikToku nakręcony w pracy lub post na Facebooku, który ktoś uznał za obraźliwy.

Rozważmy przypadki z lat 2020 i 2021:

- Stan Maryland zwolnił Arthura Love'a, który zamieścił na swoim Facebooku posty wspierające Kyle'a Rittenhouse'a. Love był zastępcą dyrektora Biura Inicjatyw Społecznych stanu Maryland. Zwolnienie było spowodowane tym, że posty zawierały „obrazy i wyrażenia dzielące społeczeństwo". Love pozwał stan Maryland, który według niego naruszył jego prawa. Pozywający twierdzi, że nie powinien być karany za treści tworzone w prywatnym czasie i publikowane na prywatnych kontach w mediach społecznościowych.
- „Eli", barista z kawiarni Starbucks, został zwolniony po tym, jak opublikował na platformie TikTok skecz pokazujący, w jaki sposób bariści radzą sobie z roszczeniowymi klientami. Eli twierdzi, że podczas kręcenia filmu w kawiarni nie było żadnych klientów, żaden sprzęt firmy nie został uszkodzony, a nagranie zarejestrowano po zamknięciu lokalu. Starbucks jest zdania, że Eli został zwolniony, ponieważ od wszystkich pracowników oczekuje się „tworzenia pełnego szacunku, bezpiecznego i przyjaznego środowiska". Starbucks uważa, że „poprzez publikacje na TikToku filmu, w którym pracownicy kpią sobie z klientów, Eli postąpił niezgodnie z wartościami Starbucksa".
- W sprawie *Ellis przeciwko Bank of New York Mellon Corp.* Trzeci Okręgowy Sąd Apelacyjny (Third Circuit Court of Appeals) stwierdził, że pracodawca może zwolnić pracownika na podstawie wpisów w mediach społecznościowych. Pracownica banku została zwolniona po zamieszczeniu na swoim publicznym koncie na Facebooku kilku postów, w których nawoływała do stosowania przemocy wobec protestujących. W rezultacie bank przeprowadził wewnętrzne dochodzenie, które obejmowało rozmowę z pracownikiem. Po przeprowadzeniu dochodzenia bank zwolnił Ellis za naruszenie firmowej polityki dotyczącej mediów społecznościowych. Bank uznał, że posty były „obraźliwe, świadczyły o złej ocenie sytuacji, pokazywały brak szacunku dla innych i zachęcały do brutalnych działań".

W otwartych źródłach możesz znaleźć wiele informacji przydatnych w dochodzeniu.

Uwaga

Książka *Open-Source Intelligence Techniques* Michaela Brazzella zawiera obszerną i głęboką analizę wykorzystania internetu w roli zasobu. W mojej książce przedstawiam zarys tej koncepcji, ale jeśli chcesz się jej dokładniej przyjrzeć, to polecam zajrzeć właśnie do książki Michaela.

Czy zbieranie informacji jest częścią śledztwa w sieci prowadzonego pod przykrywką? Z pewnością. Czy organizacja niebędąca organami ścigania może prowadzić śledztwo pod przykrywką, czy też taki sposób działania jest zarezerwowany jedynie dla agencji rządowych? Nie, nie jest, korporacje prowadzą takie śledztwa z różnych powodów. Może to być np. potrzeba zbadania konkurencji, próba przeprowadzenia dochodzenia w sprawie nieuprawnionego korzystania z usług lub chęć nawiązania kontaktu z cyberprzestępcami w celu ustalenia, czy planują oni zaatakować daną organizację.

Platforma do pracy pod przykrywką

Do przeprowadzenia śledztwa pod przykrywką niezbędne jest odpowiednie przygotowanie.

Zanim rozpoczniesz dochodzenie, zastanów się, jaką platformę wykorzystasz do interakcji z innymi użytkownikami sieci. Czy chcesz korzystać ze swojego prywatnego komputera stacjonarnego lub laptopa, sprzętu firmowego, czy z zupełnie nowego urządzenia? Niezależnie od tego, którą opcję wybierzesz, upewnij się, że z urządzenia zostaną usunięte wszystkie znajdujące się na nim dane, które mogłyby doprowadzić do ujawnienia prawdziwej tożsamości tajnego agenta lub nazwy organizacji. Zadbaj o to, aby na urządzeniu nie było:

- oprogramowania szpiegującego,
- złośliwego oprogramowania,
- śledzących aktywność ciasteczek,
- danych w pamięci podręcznej przeglądarki.

Jeśli na Twoim urządzeniu znajduje się którykolwiek z wyżej wymienionych elementów powiązany z Twoją prawdziwą tożsamością, to istnieje prawdopodobieństwo, że informacje te mogą doprowadzić do jej ujawnienia.

W trakcie wyboru platformy upewnij się, że wybrane rozwiązanie wspiera Twoją nową tożsamość. Na przykład jeśli udajesz elitarnego cyberprzestępcę specjalizującego się w obsłudze **interfejsu tekstowego** (ang. *command-line interface* — CLI), to nie będziesz zbyt wiarygodny, jeżeli do interakcji z innymi użytkownikami będziesz wykorzystywał jedynie **graficzny interfejs użytkownika** (ang. *graphical user interface* — GUI) systemu Windows 10.

Kolejną kwestią jest to, że jeśli Twoje działania doprowadzą do aresztowania lub postępowania na gruncie administracyjnym lub cywilnym, to platforma, z której korzystasz, będzie traktowana jako dowód. Jeśli nie usuniesz z urządzenia wszystkich danych związanych z Twoją prawdziwą tożsamością, możliwe, że informacje te zostaną użyte przeciwko Tobie. W idealnym świecie najlepszym rozwiązaniem byłoby korzystanie jedynie z nowego sprzętu. Niestety nie zawsze da się to zrobić. Jeśli korzystasz

z używanego sprzętu, to przed rozpoczęciem śledztwa musisz sformatować i ponownie zainstalować system operacyjny i wszelkie aplikacje potrzebne do przeprowadzenia śledztwa.

Po zakończeniu konfiguracji sprzętu urządzenie można wykorzystywać jedynie do prowadzenia śledztwa pod przykrywką.

Upewnij się też, że masz bezpieczne połączenie z siecią. Powinieneś np. wdrożyć rozwiązania chroniące przed złośliwym oprogramowaniem i zainstalować oprogramowanie antywirusowe monitorujące Twoją platformę i połączenie z siecią. Ponadto warto skorzystać z rozwiązań typu **VPN** (ang. *virtual private network*, pol. wirtualna sieć prywatna), które pozwolą Ci ukryć Twoją lokalizację. Poza tym VPN będzie szyfrowała ruch z Twojego urządzenia do miejsca docelowego, czyniąc go niezrozumiałym dla każdego, kto spróbuje go przechwycić. Istnieje kilka płatnych i bezpłatnych usług VPN. Możesz też utworzyć własną sieć prywatną.

Innym sposobem ochrony tożsamości jest zastosowanie sieci cebulowej, znanej również jako sieć Tor. Projekt Tor jest organizacją non profit, której misja to „ochrona praw i wolności człowieka poprzez tworzenie i wdrażanie bezpłatnych, otwartych i dostępnych dla każdego technologii wspierających anonimowość i prywatność, a także pogłębianie ich zrozumienia w nauce i życiu codziennym". Projekt Tor utrzymuje sieć Tor. Sieć Tor wykorzystuje oprogramowanie typu *open source* do tworzenia sieci warstwowej obsługiwanej przez wolontariuszy. Tor pozwala użytkownikom zachować anonimowość poprzez ochronę ich działań w sieci. Użycie sieci Tor jest konieczne, aby uzyskać dostęp do „ciemnej sieci" (ang. *dark web*).

Po skonfigurowaniu platformy kolejnym krokiem będzie utworzenie internetowej tożsamości śledczego.

Tożsamość w sieci

Czego potrzeba do utworzenia tożsamości w sieci? Skoro udajesz inną osobę, powinieneś pozostawić w sieci ślad podobny do tego zostawianego przez jej przeciętnego użytkownika. Musisz mieć pewność, że Twoja tajna tożsamość przejdzie ewentualną próbę jej kontroli.

Pierwszym krokiem w tworzeniu przykrywki jest utworzenie adresu e-mail. Najprostszym rozwiązaniem będzie założenie bezpłatnego konta u usługodawcy takiego jak Gmail lub Yahoo. Założenie konta u bezpłatnego dostawcy wymaga podania innego adresu e-mail lub numeru telefonu, który nie jest numerem typu Voice over IP (VoIP). Niektórzy dostawcy umożliwiają stworzenie jednorazowego adresu e-mail przeznaczonego do weryfikacji kont w innych serwisach.

Uwaga

Jednorazowy adres e-mail to metoda wykorzystywania unikalnych jednorazowych adresów e-mail do interakcji w sieci. Jej zaletą jest to, że jeśli adres zostanie ujawniony lub wykorzystany w nielegalnej działalności, użytkownik może się go szybko pozbyć w sposób, który nie wpłynie na jego inne działania w sieci.

Jednorazowe konta e-mail są dostępne zarówno za darmo, jak i za opłatą. Poniżej wymieniłem kilku dostawców takich usług:

- TempMail — *https://temp-mail.org/en/*.
- GuerrillaMail — *https://www.guerrillamail.com/*.
- Tutanota — *https://tutanota.com/*.
- ProtonMail — *https://protonmail.com/*.

Interfejs Guerrilla Mail pokazano na rysunku 10.1.

Rysunek 10.1. Interfejs Guerrilla Mail

Guerrilla Mail jest usługą bezpłatną. Po wejściu na stronę wygenerowana zostanie nazwa użytkownika. Masz możliwość wyboru jednej z kilku domen dla tworzonego konta pocztowego. Dostępna jest też opcja *Scramble Address*, która pozwala utworzyć alias dla jednorazowego konta.

W trakcie śledztwa pod przykrywką może pojawić się konieczność przeprowadzenia jakichś zakupów lub przekazywania pieniędzy podejrzanemu. Nie powinieneś wykorzystywać do tego celu jakichkolwiek zasobów finansowych, które mogłyby doprowadzić odbiorcę do Twojej prawdziwej tożsamości lub organizacji, dla której pracujesz. W tego typu zastosowaniach najlepszym rozwiązaniem są kryptowaluty. Kryptowaluta wykorzystuje zaszyfrowany ciąg danych, a do jej obsługi używany jest blockchain. Blockchain pełni również funkcję „rejestru", w którym w momencie przelewu zapisywana jest informacja o transakcji. W przypadku kryptowalut nie istnieje żadna scentralizowana infrastruktura odpowiadająca za utrzymanie waluty. Wszystko odbywa się w zdecentralizowany sposób gwarantujący anonimowość.

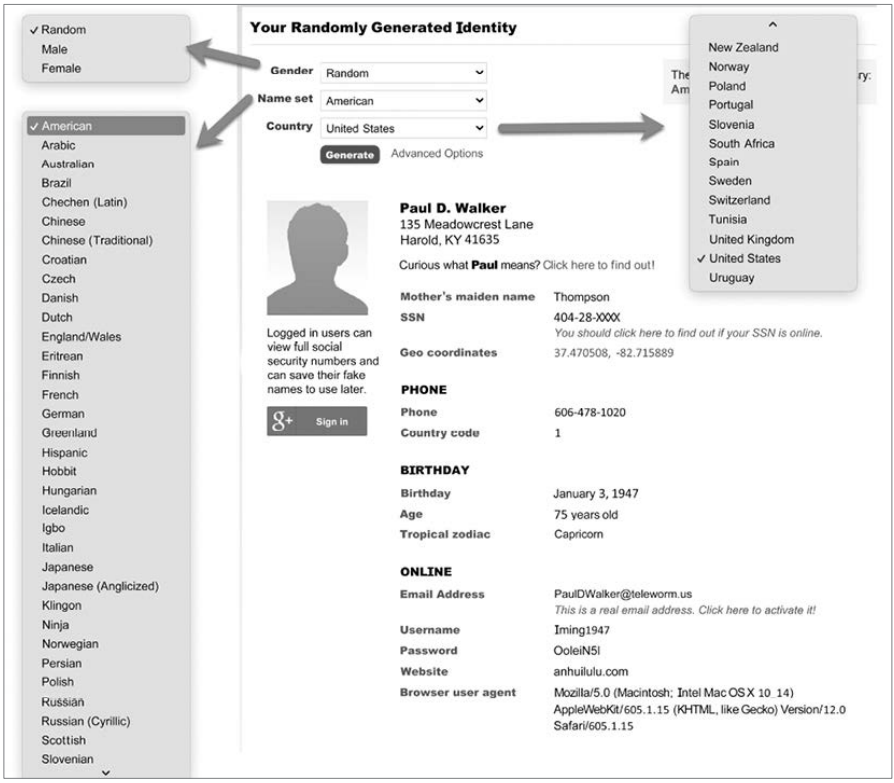
Bitcoin to zdecentralizowana, wirtualna i otwartoźródłowa waluta typu peer-to-peer, której początki sięgają 2009 r. W niektórych krajach jest uznawany za legalny środek płatniczy, a w większości państw świata administracja lokalna i centralna w pewnym stopniu dopuszcza jego stosowanie. Bitcoin stał się rozpoznawalny nawet wśród przeciętnych konsumentów i jest akceptowany przez coraz więcej organizacji. Do przechowywania bitcoinów wymagany jest tzw. portfel. Istnieje kilku dostawców oferujących portfele do przechowywania wirtualnych walut i wiele walut podobnych do bitcoina. Na przykład w 2013 r. Billy Marcus i Jackson Palmer utworzyli walutę o nazwie dogecoin. Jest ona uważana za pierwszą „walutę-mema". Powstała jako żart wyśmiewający spekulacje na rynku kryptowalut. Oficjalne logo dogecoina to głowa psa rasy shiba inu.

Śledczy pracujący pod przykrywką może skorzystać również z transakcji typu ***peer-to-peer*** (P2P). Są to zazwyczaj przelewy wykonywane za pośrednictwem aplikacji zainstalowanych na urządzeniu mobilnym lub komputerze. Przykładami takich aplikacji są Cash App, Venmo i Zelle. Aplikacje te są zwykle powiązane z kartą kredytową lub kontem bankowym użytkownika.

Inną opcją są przedpłacone karty kredytowe/debetowe, których zakup nie wymaga podawania danych osobowych.

Do generowania danych osobowych dla mojej przykrywki wykorzystuję stronę Fake Name Generator (*https://www.fakenamegenerator.com*). Witryna ta pozwala wygenerować za darmo profil zawierający imię i nazwisko, adres, adres e-mail, numer telefonu, nazwisko panieńskie matki, numery kart kredytowych i krajowe numery identyfikacyjne oraz daje możliwość dopasowania danych do dowolnego regionu, wyboru narodowości i płci. Interfejs Fake Name Generator pokazano na rysunku 10.2.

Za pomocą rozwijanych menu można wybrać płeć, zbiór imion, z którego mają być wylosowane dane, i kraj pochodzenia tworzonej osoby. Jeśli chcesz, możesz skorzystać z imion i nazwisk Amerykanów, Niemców, hobbitów, klingonów i niezmiennie popularnych ninja. Wygenerowane informacje pokazano w centralnej części rysunku 10.2.



Rysunek 10.2. Interfejs generatora Fake Name Generator

Generator stworzył osobę Paula D. Walkera zamieszkałego w stanie Kentucky. Na rysunku widzimy też numer jego telefonu, datę urodzin, znak zodiaku i niektóre artefakty sieciowe związane z jego osobą. Generator utworzył też adres e-mail wraz z nazwą użytkownika i hasłem do skrzynki pocztowej.

Na rysunku 10.3 pokazano cechy fizyczne wygenerowanej osoby, informacje o jej zatrudnieniu i numer karty kredytowej. Twórcy witryny twierdzą, że strona korzysta z generatora numerów kart kredytowych, który zwraca poprawne numery kart. Natomiast aby zapobiec oszustwom, data ważności karty jest generowana losowo, a numer CVV2 nie jest prawidłowy.

Do utworzenia nowej tożsamości przydadzą się również zdjęcia, które zwiększą naszą wiarygodność. Na stronie This Person Does Not Exist (*https://this-person-does-not-exist.com*) możesz wygenerować zdjęcia przedstawiające nieistniejące osoby. Zdjęcia są generowane losowo. Aby otrzymać inne obrazki, wystarczy odświeżyć stronę w przeglądarce.

FINANCE	
Visa	4916 4096 8823 0356
Expires	7/2026
CVV2	818
EMPLOYMENT	
Company	Father & Son
Occupation	Oxygen therapist
PHYSICAL CHARACTERISTICS	
Height	5' 11" (180 centimeters)
Weight	205.9 pounds (93.6 kilograms)
Blood type	O-
TRACKING NUMBERS	
UPS tracking number	1Z 44F 355 58 6760 719 9
Western Union MTCN	6208789813
MoneyGram MTCN	38098536
OTHER	
Favorite color	Blue
Vehicle	2001 Nissan GT-R
GUID	daed7db8-9bab-43a5-b21b-528841a83cab
QR Code	Click to view the QR code for this identity

Rysunek 10.3. Pozostałe informacje o wygenerowanej osobie

Na rysunku 10.4 pokazano zdjęcia wygenerowane za pomocą tej strony.

Rysunek 10.4. Zbiór wygenerowanych losowo zdjęć ze strony *https://this-person-does-not-exist.com*

Kolejną rzeczą wymagającą anonimizacji jest komunikacja mobilna. Możesz zastosować kilka fizycznych i cyfrowych metod, które ochronią prawdziwą tożsamość śledczego. Wielu operatorów telefonicznych sprzedaje swoje usługi w systemie prepaid, oferując abonament na okres od jednego do trzech miesięcy, czasami również wraz z urządzeniem mobilnym. Oferta obejmuje zazwyczaj usługi głosowe i transmisję danych. Na przykład Mint Mobile (*https://www.mintmobile.com*) oferuje usługi za 15 dolarów miesięcznie. Jeśli potrzebny jest Ci również telefon, to miesięczny koszt wzrasta z 20 do 44 dolarów miesięcznie. W tej ofercie możesz wybierać spośród urządzeń OnePlus n200, Samsung Galaxy A02 oraz Apple iPhone SE.

Cyfrowym rozwiązaniem tego problemu jest Fake Caller ID (*https://fakecallerid.io*). Aplikacja działa na urządzeniach Apple'a i telefonach z systemem Android. Ceny wahają się od 9,95 dolara (60 minut) do 49,95 dolara (350 minut). Usługa pozwala utworzyć fałszywy identyfikator dzwoniącego, zmienić głos użytkownika, nagrać rozmowę i przekierować ją do poczty głosowej. Oferowane są też połączenia międzynarodowe.

Do rejestracji komunikacji głosowej przez organy ścigania niezbędna jest zgoda urzędnika sądowego na przechwytywanie komunikacji przewodowej, głosowej i elektronicznej. Załóżmy, że nie jesteś funkcjonariuszem organów ścigania. W takim przypadku musisz ustalić, czy interesujący Cię stan jest stanem jedno- czy dwustronnym (uwaga ta dotyczy Stanów Zjednoczonych, w Twojej jurysdykcji mogą obowiązywać inne przepisy dotyczące rejestracji komunikacji głosowej). W stanach jednostronnych do nagrywania wymagana jest jedynie zgoda jednej strony rozmowy. W stanach dwustronnych konieczna jest zgoda po obu stronach kanału komunikacyjnego. W Stanach Zjednoczonych jest tylko 12 stanów dwustronnych. W zależności od stanu mogą obowiązywać różne wymagania. Na przykład w Oregonie rejestracja komunikacji elektronicznej wymaga zgody tylko jednej strony, a rejestracja rozmowy twarzą w twarz — zgody obu uczestników.

Jeśli kiedykolwiek dzwoniłeś do jakiegoś sprzedawcy lub organizacji i usłyszałeś komunikat o tym, że rozmowa jest nagrywana w celach szkoleniowych, to pozostanie na linii jest traktowane jak wyrażenie zgody na nagrywanie rozmowy. Jeśli powiesz osobie po drugiej stronie, że odmawiasz nagrywania, rozmowa zostanie szybko zakończona.

Wyszukiwanie informacji o podejrzanym

Po zidentyfikowaniu potencjalnego celu śledczy powinien rozpocząć rekonesans. Konieczne jest ustalenie, jakie informacje na temat podejrzanego są dostępne w sieci i poza nią. Niektóre z interesujących nas danych to:

- identyfikatory personalne,
- fizyczna lokalizacja podejrzanego,
- aktywność w mediach społecznościowych,
- członkostwo w organizacjach branżowych i aktywność zawodowa,
- działalność w grupach internetowych.

Możesz nie mieć wystarczającej ilości informacji, aby powiązać profil w sieci z osobą fizyczną. Na przykład jeśli podejrzany ma popularne nazwisko, to odróżnienie jednego Johna Smitha od innego Johna Smitha będzie trudne. Pomóc może ustalenie adresu e-mail podejrzanego, który pozwoli przefiltrować miliony informacji na temat Johna Smitha.

Nawet jeśli masz adres e-mail, możesz nie otrzymać odpowiedzi na swoje zapytanie. Załóżmy, że podejrzany korzysta z adresu *badguy27@yahoo.com*, a w sieci nie znalazłeś żadnych informacji z nim związanych. Może to być spowodowane błędem w adresie, brakiem jakiegoś znaku lub błędem w pisowni któregoś słowa.

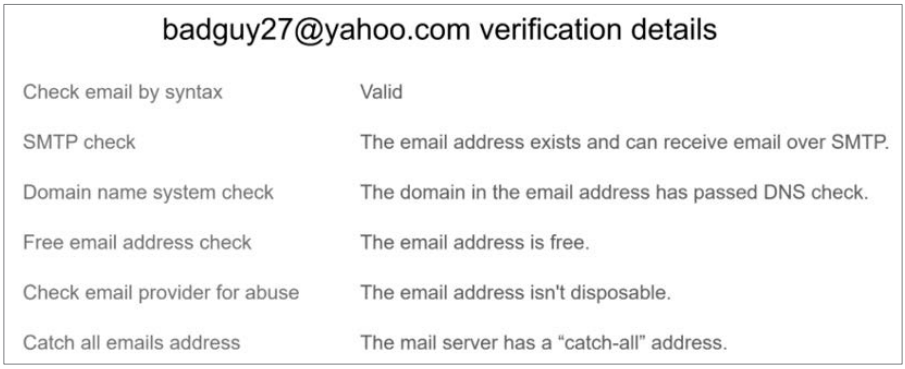
Po znalezieniu adresu kolejnym krokiem powinno być sprawdzenie jego poprawności. Istnieje wiele usług pozwalających zweryfikować adresy e-mail. Poniżej wymieniłem niektóre z nich. Część jest płatna, inne wymagają jedynie założenia darmowego konta:

- Email Hippo (*https://tools.emailhippo.com/*),
- Hunter (*https://hunter.io/*),
- Verify Email (*https://verify-email.org/*),
- DeBounce (*https://debounce.io/*),
- Emailable (*https://emailable.com/*),
- Reacher (*https://reacher.email/*),
- WhoisXML API (*https://www.whoisxmlapi.com*).

W poniższym przykładzie korzystam z usługi WhoisXML API. Na stronie wpisałem adres e-mail widoczny na rysunku 10.5.

Rysunek 10.5. Sprawdzanie poprawności adresu badguy27@yahoo.com za pomocą WhoisXML API

Adres został szybko sprawdzony. Wyniki kontroli pokazano na rysunku 10.6.



badguy27@yahoo.com verification details

Check email by syntax	Valid
SMTP check	The email address exists and can receive email over SMTP.
Domain name system check	The domain in the email address has passed DNS check.
Free email address check	The email address is free.
Check email provider for abuse	The email address isn't disposable.
Catch all emails address	The mail server has a "catch-all" address.

Rysunek 10.6. Wyniki sprawdzenia poprawności adresu badguy27@yahoo.com za pomocą WhoisXML API

Jak widzisz, adres *badguy27@yahoo.com* jest prawidłowy. Następnie warto ustalić, czy adres ten nie został ujawniony w wyniku jakiegoś wycieku. Pastebin (*https://pastebin.com/*) to strona internetowa pozwalająca tworzyć publicznie dostępne „posty" zawierające teksty wklejone przez użytkownika. Internauci często wykorzystują ją do rozpowszechniania kodów i innych treści tekstowych. Serwis można wykorzystać np.:

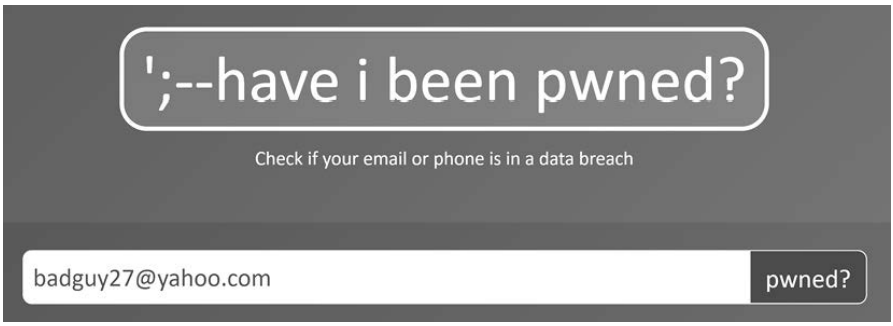
- do zamieszczania treści, które przekraczają limit znaków Twittera (w takim przypadku użytkownik może umieścić w tweecie link do pełnego tekstu umieszczonego w serwisie Pastebin);
- jako alternatywę dla Dokumentów Google;
- do promocji swojej strony internetowej;
- do udostępniania kodu źródłowego;
- do publikowania zabronionych treści;
- do udostępniania danych uzyskanych w wyniku włamań do sieci;
- do udostępniania treści/linków do darknetu (ciemnej sieci).

W serwisie Pastebin opublikowano dane uzyskane w wyniku ataków na infrastruktury firm Sony Pictures, InfraGard i Ring.

Istnieje kilka stron pozwalających sprawdzić, czy adres e-mail nie pojawił się w materiałach ujawnionych w wyniku wycieku danych. Kilka z wielu tego typu serwisów wymieniłem poniżej:

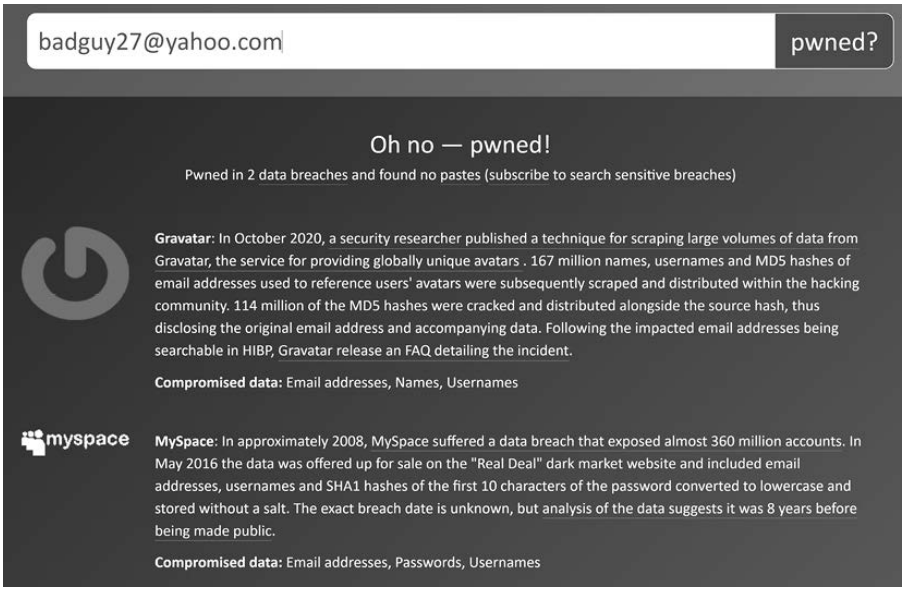
- PSBDMP (*https://psbdmp.ws/*),
- have i been pwned? (*https://haveibeenpwned.com/*),
- SpyCloud (*https://spycloud.com/*).

Na stronie *have i been pwned?* wpisałem adres e-mail *badguy27@yahoo.com*, aby ustalić, czy adres ten nie został ujawniony w jakimś ataku/włamaniu do infrastruktury sieciowej (rysunek 10.7).



Rysunek 10.7. Sprawdzenie adresu badguy27@yahoo.com w serwisie have i been pwned?

Na rysunku 10.8 widać, że adres e-mail *badguy27@yahoo.com* został ujawniony w dwóch naruszeniach danych: w wycieku danych z serwisu MySpace w 2008 r. i w wycieku danych z danych Gravatar w 2020 r.



Rysunek 10.8. Wyniki sprawdzenia adresu badguy27@yahoo.com w serwisie have i been pwned?

Ustaliliśmy już, że adres e-mail jest prawidłowy i że pojawił się w dwóch wyciekach danych. Jeśli bierzesz udział w sprawie karnej, w trakcie której odbywa się wysłuchanie stron, to obrońca strony przeciwnej może wykorzystać fakt ujawnienia danych w wycieku na swoją korzyść. To, że adres e-mail wyciekł w wyniku naruszenia bezpieczeństwa danych, nie oznacza z automatu, że ktoś uzyskał dostęp do związanej z nim skrzynki pocztowej. Jeśli próbujesz się dostać do urządzeń cyfrowych podejrzanego, upewnij się, że nie zostały one wcześniej zhakowane.

Musisz działać proaktywnie i wykluczyć linię obrony mówiącą o hakerze, który uzyskał dostęp do konta podejrzanego.

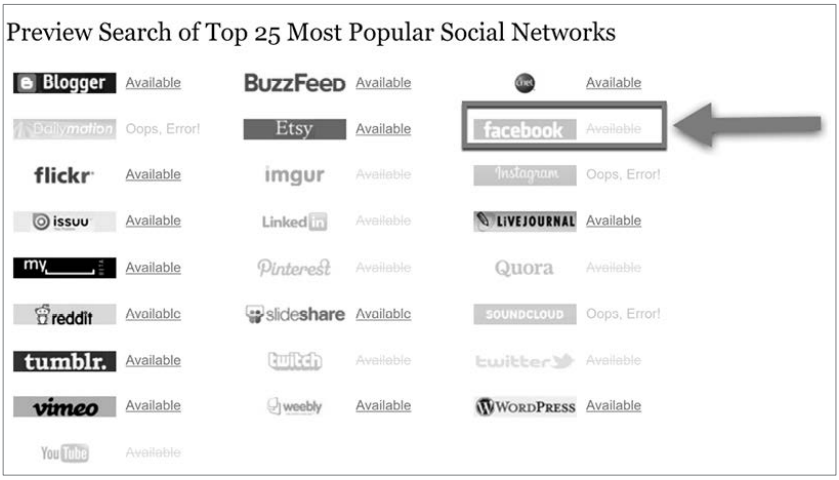
Do identyfikacji potencjalnego celu śledczy może wykorzystać również nazwę użytkownika. Często zdarza się, że użytkownicy korzystają z tej samej nazwy w różnych serwisach. Na przykład osoba używająca adresu *badguy27@yahoo.com* może stosować nazwę *bad guy 27* także u innych dostawców poczty elektronicznej, takich jak Gmail lub AOL. Użytkownik może posługiwać się tą nazwą też w mediach społecznościowych, takich jak Facebook, Instagram czy TikTok. Z tego powodu w trakcie poszukiwania informacji o podejrzanym warto sprawdzić nazwę *bad guy 27* i rozmaite jej odmiany.

Knowem (*knowem.com*) to strona internetowa umożliwiająca sprawdzanie nazw użytkowników na wielu różnych platformach. Oficjalnym celem witryny jest umożliwienie użytkownikom sprawdzenia, czy ich znak towarowy, prawa autorskie lub nazwa marki nie są wykorzystywane bez ich zgody (rysunek 10.9).

Rysunek 10.9. Wyszukiwanie frazy badguyneedslove na stronie Knowem

Po wprowadzeniu nazwy użytkownika i rozpoczęciu wyszukiwania rozpocznie się przeszukiwanie mediów społecznościowych i innych stron internetowych. Serwis poinformuje Cię, czy w danym serwisie można założyć konto o takiej nazwie użytkownika (komunikat *available*). Przekreślone słowo *available* zapisane szarą czcionką oznacza, że szukana nazwa użytkownika jest używana w danej witrynie.

Na rysunku 10.10 możesz zobaczyć, że w kilku serwisach istnieje możliwość założenia konta z nazwą użytkownika *badguyneedslove*. Podczas śledztwa interesują nas strony internetowe, przy których słowo *available* będzie wyszarzone, tak jak np. we wpisie dotyczącym Facebooka.



Rysunek 10.10. Wyniki wyszukiwania nazwy badguyneedslove w serwisie Knowem

Po dodaniu nazwy użytkownika do adresu URL Facebooka otrzymasz link *www.facebook.com/badguyneedslove* (rysunek 10.11) prowadzący do potencjalnego profilu podejrzanego.

Rysunek 10.11. Profile podejrzanego w serwisach Facebook i Twitter

Z pewnością możliwe jest wyszukiwanie osób również za pośrednictwem wyszukiwarki Google. W jej przypadku musisz być po prostu przygotowany na konieczność przeglądania wyników wyszukiwania w nadziei, że trafisz na swój cel. Istnieją też wyszukiwarki zaprojektowane specjalnie do poszukiwania osób. Wyszukiwarki te zazwyczaj umożliwiają uzyskanie podstawowych informacji o szukanej osobie, a następnie żądają opłaty przed przedstawieniem jakichkolwiek bardziej szczegółowych danych. Zalecam korzystanie z wielu wyszukiwarek. Dzięki temu będziesz miał pewność, że otrzymasz najlepsze dostępne informacje. Z mojego doświadczenia wynika, że dokładność wyników zmienia się w zależności od wyszukiwarki. Dlatego staram się zapisać wyniki wszystkich wyszukiwań w jednym dokumencie.

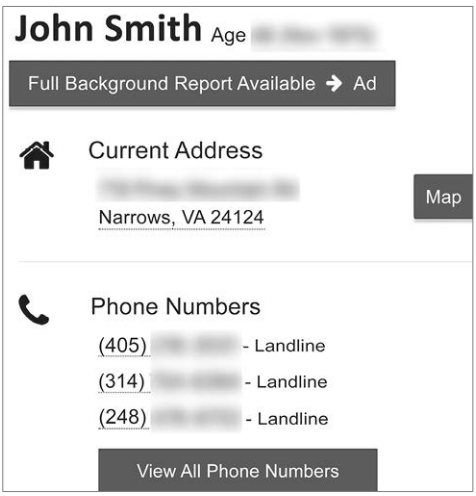
Za pomocą wyszukiwarek osób udało mi się znaleźć aktualne i poprzednie adresy podejrzanych, ich aktualne i przeszłe numery telefonów stacjonarnych oraz komórkowych, informacje o członkach ich najbliższej i dalszej rodziny, aktualne i archiwalne numery kont bankowych oraz daty urodzin. W niektórych przypadkach zdołałem również ustalić okręgi wyborcze i dane sąsiadów.

Wyszukiwanie rozpoczynam zazwyczaj od True People Search (*https://truepeople*
↪search.com/) (rysunek 10.12).

Rysunek 10.12. True People Search — ekran wyszukiwania

W True People Search masz możliwość wyszukiwania według nazwiska, numeru telefonu lub adresu.

W wynikach wyszukiwania znajdziesz imię i nazwisko osoby, jej wiek i rok urodzenia, aktualny adres i numery telefonów. Możesz również wyświetlić mapę pokazującą aktualny adres, a także uzyskać wszystkie numery telefonów powiązane z daną osobą (rysunek 10.13).

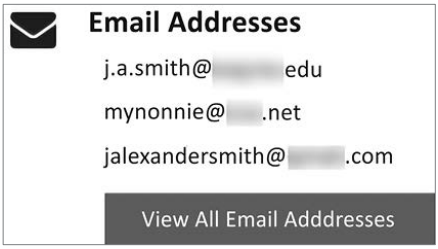


Rysunek 10.13. Wyszukiwarka True People Search — wyniki wyszukiwania (imię i nazwisko)

Poniżej zobaczysz poprzednie adresy związane z daną osobą. Adresy zawierają nazwę ulicy, miasto, stan i kod pocztowy. Widoczny jest także miesiąc i rok, w którym adres był powiązany z daną osobą (rysunek 10.14).

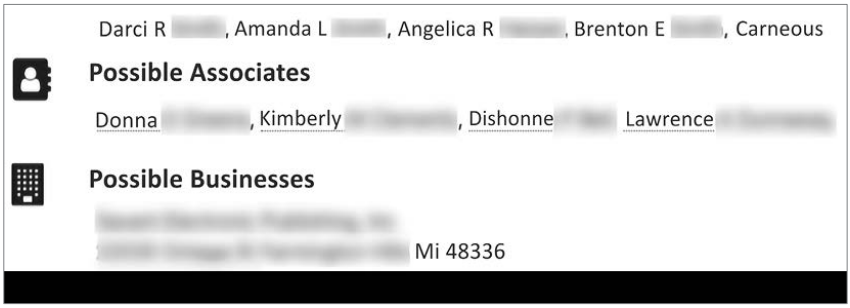
Rysunek 10.14. Wyszukiwarka True People Search — wyniki wyszukiwania (adres zamieszkania)

W kolejnych polach zobaczysz aktualne adresy e-mail. Wyszukiwarka nie podaje dat korzystania z adresów e-mail, co utrudnia ustalenie, czy użytkownik nadal używa tych kont. Za pomocą przycisku możesz wyświetlić dodatkowe adresy e-mail, które mogą być powiązane z daną osobą. Pamiętaj, że musisz samodzielnie zweryfikować te dane — nie ma żadnej gwarancji, że wyniki te odnoszą się do osoby, której szukasz. Podczas poszukiwań możesz trafić na nieprawdziwe dane dotyczące podejrzanego (rysunek 10.15).



Rysunek 10.15. Wyszukiwarka True People Search — wyniki wyszukiwania (adres e-mail)

Pod koniec raportu (rysunek 10.16) znajdziesz listę potencjalnych krewnych, współpracowników i firm związanych z szukaną osobą. Informacje te możesz wykorzystać, aby potwierdzić lub zaprzeczyć, że widoczne w serwisie dane odnoszą się do osoby będącej przedmiotem Twojego śledztwa.



Rysunek 10.16. Wyszukiwarka True People Search — wyniki wyszukiwania (możliwe powiązania)

Istnieje mnóstwo usług umożliwiających wyszukiwanie osób. Jest ich o wiele za dużo, abym mógł je opisać w tej książce. Po zapoznaniu się z ich listą możesz rozpocząć tworzenie listy swoich ulubionych wyszukiwarek.

Jak już wspomniałem, True People Search jest jedną z pierwszych wyszukiwarek, z których korzystam. Poniżej wymieniłem kilka kolejnych pozwalających uzyskać podobne informacje. Zwracane przez nie wyniki będą się częściowo pokrywały. Dokładnie je przeanalizuj, aby ustalić, czy podane informacje dotyczą osoby, której szukasz. Oto kilka innych wyszukiwarek, których używałem w przeszłości:

- Whitepages — *https://www.whitepages.com/*.
- ZabaSearch — *https://zabasearch.com/*.
- People Search Now — *https://peoplesearchnow.com/*.
- Spokeo — *https://www.spokeo.com/*.

W kolejnym podrozdziale pokażę Ci, jak zapisać czynności wykonywane w toku śledztwa w sieci, tak abyś mógł właściwie udokumentować cały proces i przedstawić swoje dowody w postępowaniu administracyjnym lub sądowym.

Rejestracja czynności wykonywanych w toku śledztwa w sieci

Czy można powiedzieć, że przeprowadziłeś śledztwo, jeśli nie udokumentowałeś swoich czynności? Umiejętność rejestrowania wysiłków dochodzeniowych jest równie ważna jak samo śledztwo. Wykonane czynności musisz udokumentować w raporcie z wynikami. Musisz w nim uwzględnić zarówno pozytywne, jak i negatywne wyniki. W trakcie śledztwa w sieci należy dokumentować przeprowadzane czynności. Możesz to robić

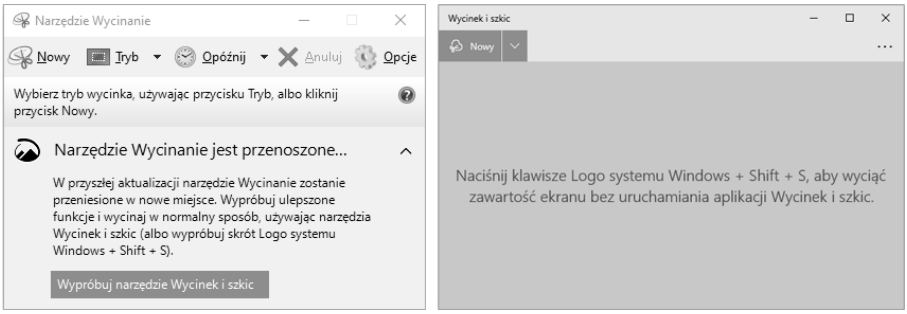
w czasie rzeczywistym podczas prowadzenia działań lub odtwarzać wykonane czynności w późniejszym czasie.

Skuteczną metodą przechwytywania zawartości ekranu jest robienie jego zrzutów. Zrzut ekranu musi się skupiać na przechwyconym artefakcie lub działaniu, które chcesz udokumentować. W trakcie wykonywania zrzutu na ekranie powinno znajdować się to, co chcesz udokumentować. Na przykład zrzut ekranu z otwartymi sześcioma lub siedmioma oknami nie przekazuje istotnych informacji w efektywny sposób. Zarówno macOS, jak i Windows zawierają natywne narzędzia do przechwytywania zawartości ekranu.

W systemie macOS możesz uruchomić wyszukiwarkę Spotlight, naciskając jednocześnie klawisze *command* i *spacja* (rysunek 10.17).

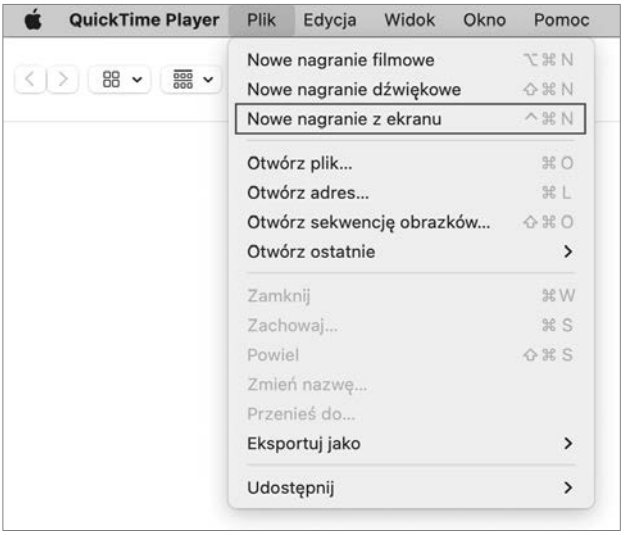
Rysunek 10.17. Wyszukiwarka Spotlight — „zrzut ekranu"

W systemie Windows dostępne jest narzędzie *Wycinanie*, obecnie zastępowane przez narzędzie *Wycinek i szkic*. Oba narzędzia mają tę samą funkcjonalność. Na rysunku 10.18 pokazano ich interfejsy.



Rysunek 10.18. Microsoft Windows — narzędzia Wycinanie oraz Wycinek i szkic

Możesz też nagrać wideo prezentujące wykonywane przez Ciebie czynności. W systemie macOS dostępne jest darmowe narzędzie QuickTime Player (rysunek 10.19). QuickTime Player pozwala nagrywać wideo za pomocą kamery podłączonej do portu USB i tworzyć nagrania zawartości ekranu. Jeśli rejestrujesz także dźwięk, upewnij się, że Twoi współpracownicy znajdujący się w pobliżu wiedzą, że prowadzisz nagranie. Wyobraź sobie, jak będziesz sfrustrowany, gdy jeden z nieświadomych nagrywania kolegów głośno przeklnie w trzydziestej minucie nagrania, które ma trafić do sądu.



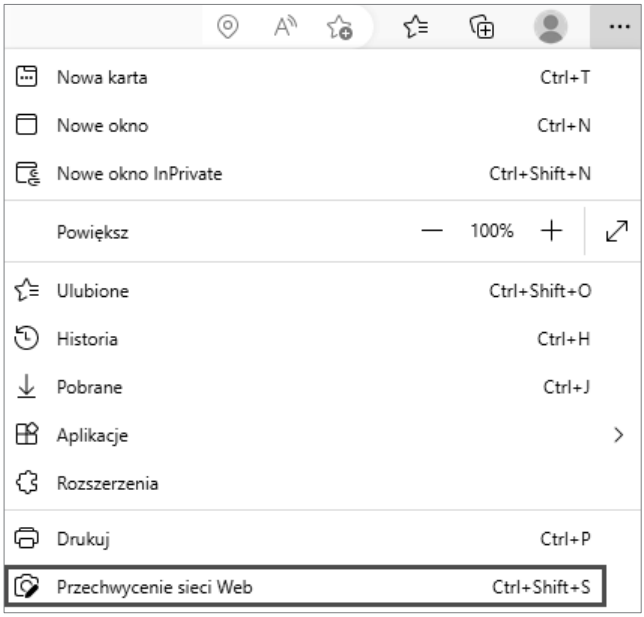
Rysunek 10.19. Menu programu QuickTime Player

W systemie Microsoft Windows możesz rozpocząć nagrywanie ekranu za pomocą kombinacji *Windows+Alt+R*. Po jej wybraniu na ekranie pojawi się mały widżet nagrywania. Aby zatrzymać nagrywanie, możesz ponownie wywołać kombinację *Windows+Alt+R* lub kliknąć lewym przyciskiem myszy przycisk „stop" znajdujący się w widżecie. Po zatrzymaniu nagrywania na ekranie pojawi się powiadomienie, że *Klip z gry został nagrany*. System zapisze wideo w folderze *Wideo/Przechwycone* w katalogu użytkownika.

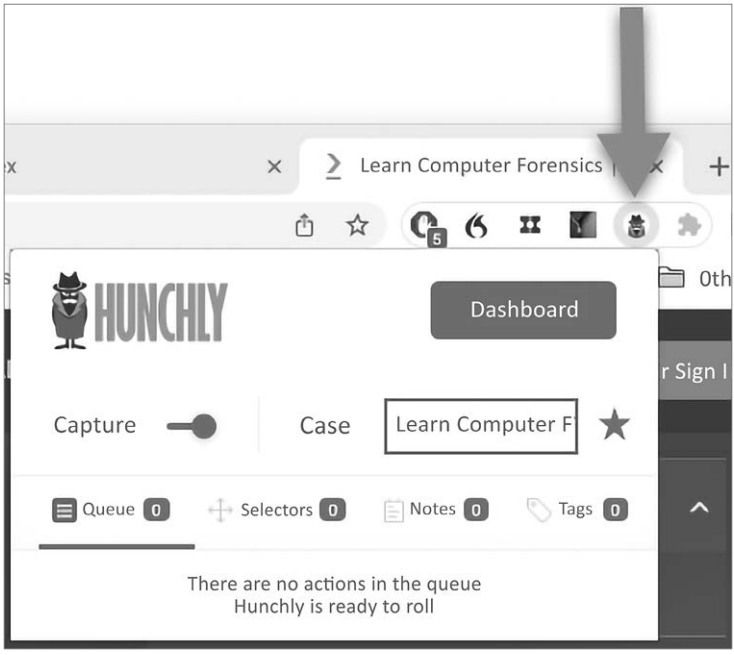
Przeglądarka Edge ma możliwość zapisania odwiedzonych stron internetowych. Interfejs przeznaczony do przechwytywania ich zawartości możesz wyświetlić za pomocą skrótu *Ctrl+Shift+S* (rysunek 10.20).

Innym sposobem zapisu danych wyświetlanych w przeglądarce jest użycie programu Hunchly (*https://www.hunch.ly/*). Często zdarza się, że śledczy rozpoczyna pracę od jednej karty w przeglądarce. Z czasem w przeglądarce otwierane są kolejne karty, aż wkrótce w tym samym oknie otwartych jest wiele zakładek dotyczących różnych wątków śledztwa. Jeśli śledczy nie sporządził odpowiednich notatek/dokumentacji, cofnięcie się i odtworzenie wykonanych może być trudne. Hunchly pomaga rozwiązać ten problem. Narzędzie to współpracuje z przeglądarką Chrome i wymaga zainstalowania aplikacji Hunchly.

Podczas instalacji aplikacji instalowane jest też rozszerzenie do przeglądarki (rysunek 10.21).



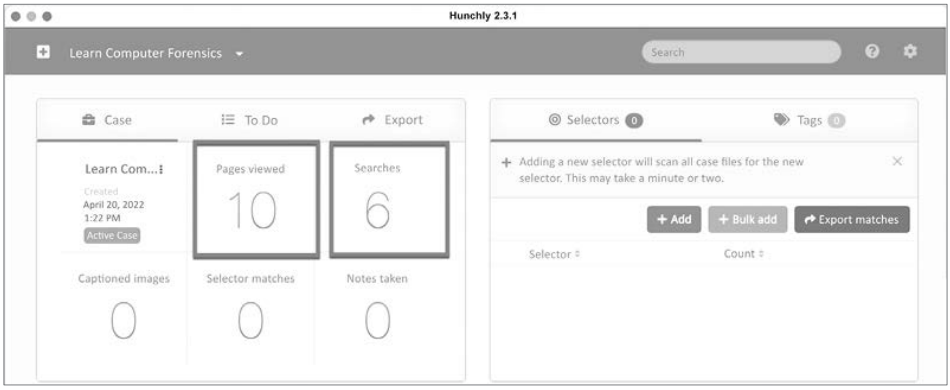
Rysunek 10.20. Menu przechwytywania w przeglądarce Edge



Rysunek 10.21. Menu rozszerzenia Hunchly w przeglądarce Chrome

Hunchly oferuje bezpłatną 30-dniową wersję próbną. Po zakończeniu okresu próbnego możesz zakupić roczną licencję oferowaną w bardzo rozsądnej cenie.

Po aktywacji Hunchly za pośrednictwem rozszerzenia w przeglądarce program rozpocznie monitorowanie aktywności w oknie przeglądarki. Jeśli otworzysz dodatkowe karty, Hunchly zarejestruje również ich zawartość. Na rysunku 10.22 pokazano pulpit narzędzia (*Dashboard*), w którym możesz zobaczyć aktywną sprawę (*Case*) wraz z informacjami o liczbie odwiedzonych stron (*Pages viewed*) i przeprowadzonych wyszukiwań (*Searches*). W trakcie testowania narzędzia odwiedziłem dziesięć stron internetowych i przeprowadziłem sześć wyszukiwań.



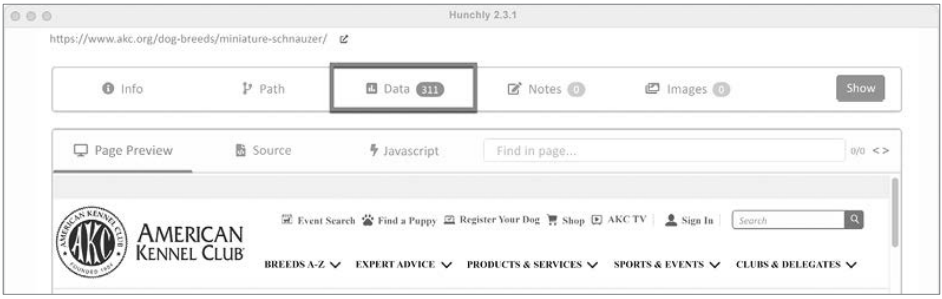
Rysunek 10.22. Pulpit Hunchly

Jedną z witryn, które odwiedziłem, była strona *American Kennel Club (AKC)*, na której przejrzałem informacje na temat miniaturowych sznaucerów. Przeprowadziłem też kilka wyszukiwań zdjęć miniaturowych sznaucerów w wyszukiwarce Google. Na rysunku 10.23 pokazano zrzut ekranu zawierający informacje o odwiedzonych przeze mnie stronach, wraz z datami i ze znacznikami czasu.

Hunchly zapamiętuje nie tylko wizualne elementy strony internetowej, ale również umieszczone na niej dane, takie jak adresy e-mail, adresy IP, dane Google Analytics, a w niektórych przypadkach także współrzędne GPS. Na rysunku 10.24 pokazano podgląd strony American Kennel Club wyświetlony w tym programie. W samym środku menu widocznego nad stroną znajduje się przycisk *Data* (dane).

W tym przykładzie narzędzie pozyskało z tej strony 311 wpisów. Na rysunku 10.25 możesz zobaczyć wpisy dotyczące Google Analytics i narzędzi śledzących Facebooka oraz adresy e-mail i adresy IP. Wszystkie te informacje znajdowały się w tej witrynie.

Rysunek 10.23. Hunchly — historia przeglądanych stron



Rysunek 10.24. Hunchly — podgląd strony

Hunchly pozwala również wyeksportować przechwycone dane do plików PDF. Opcja ta może się przydać, gdy będziesz chciał rozpowszechnić fizyczne kopie zebranych przez siebie dowodów.

Hunchly to tylko jedno z wielu narzędzi, które umożliwiają przechwytywanie stron internetowych. Zamiast niego możesz skorzystać z jednej z poniższych opcji:

- FireShot — *https://getfireshot.com/*.
- HTTrack — *https://www.httrack.com/*.
- Web2Disk — *http://www.web2disk.com/*.
- SiteSucker — *https://ricks-apps.com/osx/sitesucker/index.html*.
- X1 Social Discovery — *https://www.x1.com/products/x1-social-discovery/*.
- EyeWitness — *https://github.com/FortyNorthSecurity/EyeWitness*.
- FAW — *https://en.fawproject.com*.

Rysunek 10.25. Hunchly — widok danych

Powyższa lista nie zawiera wszystkich istniejących narzędzi. Prawdopodobnie istnieją też inne programy oferujące te same funkcjonalności. Korzystanie z niektórych narzędzi jest bezpłatne, niektóre są niedrogie, a niektóre bardzo drogie. Wybór zależy od sytuacji. Nie ma znaczenia, jakiego narzędzia używasz. Niektóre płatne narzędzia oferują te same funkcjonalności co bezpłatne programy. Pamiętaj, że w przypadku płatnych rozwiązań w cenę wliczono obsługę klienta. W przypadku problemów z bezpłatnym programem będziesz musiał sam znaleźć rozwiązanie. Ostatecznie celem jest osiągnięcie biegłości w korzystaniu ze swoich ulubionych narzędzi. Musisz także zrozumieć, jakie czynności wykonują te programy pod ich interfejsem graficznym.

Podsumowanie

W tym rozdziale omówiłem śledztwa w sieci. Przyjrzeliśmy się działalności pod przykrywką i sposobom tworzenia fałszywych tożsamości, z których może korzystać śledczy. W trakcie śledztwa w sieci nigdy nie powinieneś używać swojej prawdziwej tożsamości. Jeśli to zrobisz, a podejrzany będzie w stanie ustalić Twoje dane, narazisz się na niebezpieczeństwo. Przyjrzeliśmy się też rozmaitym możliwościom szukania informacji na temat podejrzanych. Podejrzany mógł nie zostawić po sobie żadnego cyfrowego śladu, ale jest to bardzo mało prawdopodobne. Korzystając z publicznie dostępnych informacji, możesz zebrać dane na temat podejrzanego bez wzbudzania

jego czujności. Musisz udokumentować wszystkie wykonywane działania. Możesz do tego wykorzystać zrzuty ekranu i nagrania wideo. Możesz też zapisać zawartość odwiedzanych stron internetowych. Po przeczytaniu tego rozdziału powinieneś być w stanie:

- Wymienić sposoby wyszukiwania informacji personalnych w sieci.
- Określić, w jaki sposób prowadzi się śledztwa w sieci.
- Ustalić, jak zapisać czynności wykonywane w sieci, filmy wideo, zdjęcia i inne ważne dla sprawy treści.

W następnym rozdziale omówię podstawy sieci komputerowych. Poznanie sposobu, w jaki przesyła się dane przez internet, ma kluczowe znaczenie dla zrozumienia, gdzie szukać artefaktów, które pomogą Ci udowodnić lub obalić zarzuty postawione podejrzanemu.

Pytania

1. Aby przeprowadzić śledztwo w sieci, musisz być funkcjonariuszem organów ścigania.
   a. Prawda.
   b. Fałsz.
2. Wykorzystanie którego z poniższych elementów należy rozważyć w pierwszej kolejności przed rozpoczęciem śledztwa sieciowego pod przykrywką?
   a. RAM.
   b. System operacyjny.
   c. Tablet.
   d. Narzędzia szyfrujące.
3. Które z poniższych elementów należy usunąć z platformy do prowadzenia działań pod przykrywką?
   a. Oprogramowanie szpiegujące.
   b. Złośliwe oprogramowanie.
   c. Facebooka.
   d. Ciasteczka.
4. Co można wykorzystać do ukrycia swojej lokalizacji?
   a. Wi-fi w Starbucksie.
   b. Konto gościa.

c. Wirtualne sieci prywatne.

d. Przeglądarkę Mosaic.

5. Która z poniższych firm oferuje jednorazowe adresy e-mail?

a. Temp Mail.

b. Tal Shiar Mail.

c. Secret Mail.

d. Section 31 Mail.

6. Która z poniższych walut jest wirtualną walutą typu peer-to-peer istniejącą od 2009 r.?

a. Trekcoin.

b. Dogecoin.

c. Bytecon.

d. Bitcoin.

7. Kto może upoważnić organy ścigania do przechwytywania komunikacji przewodowej, ustnej i elektronicznej?

a. Sędzia.

b. Admirał.

c. Gubernator.

d. Do wykonywania tych czynności nie jest potrzebne żadne pozwolenie.

8. Jaką usługę świadczy Hippo Email?

a. Weryfikację adresów e-mail.

b. Weryfikację treści e-maili.

c. Weryfikację nadawców wiadomości e-mail.

d. Sprawdzanie lokalizacji skrzynki odbiorczej.

9. Co nie jest powodem, dla którego ktoś może chcieć skorzystać z serwisu Pastebin?

a. Publikacja treści przekraczającej limit znaków na Facebooku.

b. Promocja witryny.

c. Udostępnianie kodu źródłowego.

d. Publikowanie zabronionych materiałów.

10. Do przeprowadzenia wyszukiwania w True People Search niezbędna jest zgoda sędziego.
    a. Prawda.
    b. Fałsz.

Materiały dodatkowe

M. Bazzell, *Open source intelligence techniques: Resources for searching and analyzing online information*, USA, *Inteltechniques.com*, 2018.

V. Troia, *Hunting cyber criminals: A hacker's guide to online intelligence gathering tools and techniques*, Indianapolis, Indiana: John Wiley & Sons Inc., 2020.

Informatyka śledcza: Twoja tajna broń!

Aby ująć i ukarać cyberprzestępcę, potrzeba czegoś więcej niż odnalezienie śladów włamania. Informatyk śledczy musi nie tylko prowadzić badania, ale również pozyskiwać i zabezpieczać dowody cyfrowe. Powinien też biegle je analizować i pisać raporty w taki sposób, aby można było z nich skorzystać w postępowaniu sądowym. Cała ta praca musi być wykonywana zgodnie z zasadami informatyki śledczej.

To drugie wydanie popularnego przewodnika dla śledczych. Dzięki niemu sprawnie przygotujesz się do pracy z narzędziami kryminalistycznymi i zapoznasz się ze stosowanymi w informatyce śledczej technikami. Nauczysz się pozyskiwać informacje o podejrzanych i zabezpieczać znajdujące się w sieci dane, które mogą się okazać istotne w wyjaśnieniu sprawy. Zdobędziesz także potrzebną wiedzę o topologiach sieciowych, urządzeniach i niektórych protokołach sieciowych. Bardzo ważnym elementem publikacji jest rozdział poświęcony zasadom tworzenia raportów kryminalistycznych. Cenne informacje i wskazówki zawarte w przewodniku pomogą Ci odnieść sukces w dochodzeniach korporacyjnych lub śledztwach w sprawach karnych.

W książce:

- proces dochodzeniowy i zasady pracy z dowodami
- walidacja narzędzi, oprogramowania i metod badawczych
- tworzenie i walidacja sterylnych nośników
- odkrywanie i analiza artefaktów
- przechwytywanie zawartości pamięci RAM
- analiza osi czasu, mediów, ciągów znaków i odzyskiwanie usuniętych plików

William Oettinger jest emerytowanym oficerem policji 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.

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 978-83-289-0171-1
9 788328 901711
Cena: 79,00 zł
packt