Helion

<packt>

WYDANIE III

Informatyka śledcza

Narzędzia i techniki skutecznego reagowania na incydenty bezpieczeństwa

GERARD JOHANSEN

Tytuł oryginału: Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response, 3rd Edition

Tłumaczenie: Piotr Fabijańczyk

ISBN: 978-83-289-0432-3

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/obrcyb
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

CZĘŚĆ 2. Pozyskiwanie dowodów

CZĘŚĆ 3. Badanie dowodów

CZĘŚĆ 4. Reagowanie na incydenty związane z oprogramowaniem ransomware

Rozdział 3

Podstawy kryminalistyki cyfrowej

Kryminalistykę można zdefiniować jako stosowanie zasad naukowych w sprawach prawnych. W przypadku incydentu członkowie zespołu **CSIRT** (**zespół reagowania na incydenty związane z bezpieczeństwem komputerowym**) mogą zostać poproszeni o przeprowadzenie analizy dowodów cyfrowych uzyskanych podczas incydentu z wykorzystaniem narzędzi, technik i wiedzy z zakresu kryminalistyki cyfrowej. Aby mieć pewność, że dowody są przetwarzane prawidłowo i będą mogły zostać dopuszczone podczas rozprawy sądowej, eksperci ds. kryminalistyki cyfrowej muszą rozumieć kwestie prawne, a także szczegółowe punkty procesu kryminalistyki cyfrowej.

W tym rozdziale przyjrzymy się przepisom prawnym mającym wpływ na działania zespołu CSIRT i ekspertów ds. kryminalistyki cyfrowej, a także omówimy zasady regulujące dopuszczanie dowodów w sądzie. Aby zapewnić odpowiedni kontekst dla podejmowanych działań, przeanalizujemy również proces kryminalistyki cyfrowej i wreszcie zajmiemy się infrastrukturą niezbędną podczas włączania kryminalistyki cyfrowej do zespołu CSIRT.

W tym rozdziale omówimy następujące tematy:

- Rozwój kryminalistyki.
- Zasada wymiany Locarda.
- Zagadnienia prawne w kryminalistyce cyfrowej.
- Procedury kryminalistyczne podczas reagowania na incydenty.

Rozwój kryminalistyki

W ciągu ostatnich 20 lat byliśmy świadkami gwałtownego wzrostu zainteresowania kryminalistyką. Mówiąc najprościej, kryminalistyka dotyczy zastosowania metod naukowych w sprawach prawnych. Rzeczywista praktyka kryminalistyki polega na zbieraniu fizycznych i cyfrowych dowodów w procesie analizy, a następnie przedstawianiu wyników naukowych w sądzie. Pomimo tego, że proces ten jest przedstawiany w popularnych mediach, kryminalistyka jest w istocie procesem bardzo szczegółowym i czasochłonnym, który wymaga stosowania dobrze przemyślanych procedur, technik i korzystania z doświadczenia.

Kryminalistyka stała się integralną częścią wielu dyscyplin, nawet tych spoza zakresu wymiaru sprawiedliwości. Na przykład badacze wypadków lotniczych wykorzystują techniki kryminalistyczne do badania przyczyn awarii samolotów. Podobne zasady i techniki są stosowane podczas prowadzenia dochodzeń w sprawie podejrzeń o defraudację i pranie pieniędzy. Techniki kryminalistyczne są wykorzystywane nawet do weryfikacji autentyczności dzieł sztuki, w związku z dużą liczbą falsyfikatów.

Pierwszą głośną sprawą, w której kryminalistyka odegrała istotną rolę, były morderstwa Kuby Rozpruwacza pod koniec XIX wieku. Śledczym z londyńskiej policji metropolitalnej udało się zidentyfikować, zebrać, a następnie zbadać fizyczne dowody pozostawione przez nieznanego sprawcę. Mniej więcej w tym czasie do rosnącego zasobu wiedzy i praktyk dodano dwie inne wypróbowane praktyki kryminalistyczne, którymi były porównanie odcisków palców i fotografie wykonane na miejscu zbrodni.

Praktyki te rozwijały się powoli na bazie dostępnej technologii aż do zakończenia drugiej wojny światowej. W tym siedemdziesięciopięcioletnim okresie pojawiła się kolejna bardzo użyteczna metoda, jaką było identyfikowanie sprawców na podstawie DNA. Kryminalistyka była też stosowana do badania śladów narzędzi i balistyki. W drugiej połowie XX wieku kryminalistyka cyfrowa zaczęła też odgrywać rolę w różnych dyscyplinach medycyny sądowej.

Zasada wymiany Locarda

Kluczową zasadą w kryminalistyce jest **zasada wymiany Locarda**. Doktor Edmond Locard był pionierem w dziedzinie kryminalistyki. Jego wkład w tę dziedzinę sprawił, że wielu uznawało go za francuskiego Sherlocka Holmesa. Zasada Locarda, mówiąc najprościej, opiera się na założeniu, że w każdym momencie kontaktu ze światem fizycznym pozostawiany jest ślad. Na przykład włamywacz wybija okno, by dostać się do domu. Następnie przeciska się przez to okno i zaczyna zabierać otaczające go przedmioty. Zgodnie z zasadą wymiany Locarda włamywacz pozostawi na dywanie ślady brudu z butów. Na różne powierzchnie w domu mogą spadać jego włosy lub naskórek. Jeśli włamywacz nie stosował rękawiczek, to mógł również zostawić odciski palców na klamkach drzwi.

Ta wymiana działa w dwóch kierunkach. Podobnie jak włamywacz zostawia swoje ślady w całym domu, tak samo ślady domu zostają na nim. Do jego butów mogą przyczepić się włókna dywanu. Fragmenty wybitych szyb mogą wbić się w obuwie oraz pozostać na ubraniu włamywacza. Te ślady umożliwiają powiązanie go z miejscem zdarzenia.

Zasada ta obowiązuje od momentu pierwszej przestępczej aktywności. Tym, co się zmieniło, jest zdolność naukowców zajmujących się kryminalistyką i praktyków kryminalistyki do wykrywania i analizowania tych śladów. Na przykład dowody DNA istnieją od czasu, gdy Kain zabił Abla. Jednak dopiero niedawno stały się przydatne podczas prowadzenia dochodzenia. Metody i technologie rozwinęły się do tego stopnia, że naukowcy z zakresu medycyny sądowej mogą definitywnie udowodnić, że materiał biologiczny można powiązać z konkretną osobą z wyłączeniem każdego innego człowieka.

W przypadku zasady Locarda należy pamiętać o kilku kwestiach. Po pierwsze, istnieje duże zróżnicowanie w zakresie tego, w jak długim czasie można odszukać dowody śladowe. Na przykład niektóre ślady, takie jak ślady narzędzi pozostawione po użyciu łomu do wyważenia drzwi, mogą utrzymywać się przez miesiące, a nawet lata. Natomiast odciski palców wystawione na działanie żywiołów stają się nieprzydatne już po kilku dniach, a nawet godzinach. Po drugie, należy przestrzegać pewnych procesów, które zapewniają integralność dowodów śladowych. Jeśli dowody śladowe nie zostaną odpowiednio zebrane, to mogą zostać zmienione lub zniszczone, co czyni je całkowicie bezużytecznymi do celów dochodzeniowych. Po trzecie, musi istnieć odpowiednia technologia użyteczna podczas analizy tych śladów. DNA istnieje od zarania życia na Ziemi, jednak możliwość wykorzystania tych śladów do celów dochodzeniowych zależy od technologii umożliwiającej właściwe porównywanie i analizowanie próbek DNA. Wreszcie, obecny jest również czynnik ludzki. Przetwarzaniem dowodów muszą zajmować się odpowiednio przeszkoleni i wykwalifikowani analitycy, którzy mogą przeglądać dane i wyciągać wnioski.

Dyskusja na temat zasady wymiany Locarda w dziedzinie kryminalistyki cyfrowej może wydawać się nieco dziwna. Jednak w rzeczywistości ta sama zasada, która leży u podstaw kryminalistyki w świecie fizycznym, ma takie samo zastosowanie w kryminalistyce cyfrowej. Na przykład proste połączenie z systemem za pomocą funkcji Microsoft Windows Remote Desktop pozostawia ślady. Załóżmy, że zewnętrzny aktor zajmujący się cyberwłamaniami uzyskał prawidłowe poświadczenia użytkownika i zdołał połączyć się za pośrednictwem ujawnionego systemu. Już samo połączenie spowodowałoby utworzenie wpisu dziennika w ujawnionym systemie. Użycie prawidłowych poświadczeń do zalogowania się do systemu spowodowałoby utworzenie drugiego wpisu w dzienniku. Taki wpis dziennika zawiera adres IP systemu atakującego. Ten adres IP może być również zawarty w dziennikach zapory sieciowej. Wpisy dziennika i potencjalnie pliki z zaatakowanego systemu zostałyby zachowane również w systemie włamywacza.

Istotą zrozumienia zasady wymiany Locarda, jest koncepcja dowodów śladowych. Cyberprzestępcy dołożą wszelkich starań, aby usunąć swoje ślady w taki sam sposób, w jaki robią to bardzo inteligentni przestępcy, jednak ciągle pozostanie po nich pewien ślad. Kluczem jest posiadanie narzędzi i możliwości wykrywania właśnie tych śladów oraz powiązania ich z podmiotem odpowiedzialnym za zagrożenie.

Zagadnienia prawne w kryminalistyce cyfrowej

Wspominaliśmy w rozdziale 1., że właściwa reakcja na incydent obejmuje kluczowe osoby reprezentujące różne dyscypliny. Uwypukla to jedno z często spotykanych nieporozumień: reagowanie na incydent jest ściśle kwestią technologiczną. Dziedziną, z którą reagowanie na incydenty jest mocno związane, jest prawo. Istnieje wiele przepisów i regulacji, które bezpośrednio wpływają na zdolność organizacji do reagowania na incydenty, począwszy od powiadamiania o naruszeniu, a skończywszy na ochronie prywatności. Przepisy te zapewniają rządom ramy ścigania przestępców, a także określają ścisłe zasady dotyczące takich kwestii jak postępowanie z dowodami i przedstawianie ich w sądzie.

Regulacje prawne

W połowie lat 80., gdy przestępczość komputerowa zaczęła stawać się coraz bardziej powszechna, zaczęto tworzyć przepisy dotyczące coraz większej liczby przypadków cyberprzestępczości. Na przykład w Stanach Zjednoczonych federalne prawo karne obejmuje określone ustawy, które bezpośrednio dotyczą działalności przestępczej z użyciem komputera:

- **18 USC § 1029 — Oszustwa i powiązane działania związane z urządzeniami dostępowymi**. Ustawa dotyczy wykorzystywania komputera do popełniania oszustw. Jest to akt prawny, na który najczęściej powołują się prokuratorzy w przypadkach, w których cyberprzestępcy wykorzystują komputer lub komputery do kradzieży tożsamości lub innych działań związanych z oszustwami.
- **18 USC § 1030 — Computer Fraud and Abuse Act** (CFAA). Spośród wielu przepisów tego aktu prawnego najbardziej związanym z reagowaniem na incydenty jest ten dotyczący nieautoryzowanego dostępu do systemu komputerowego. Prawo to odnosi się również do nielegalności ataków typu **odmowa usługi (DoS)**.
- **Electronic Communications Privacy Act** (ECPA). Jest to poprawka do federalnego statutu dotyczącego podsłuchów, która została uchwalona w roku 1986. Zgodnie z nią nieupoważnione przechwytywanie komunikacji za pośrednictwem środków elektronicznych, takich jak telekomunikacja i internet, jest nielegalne. Ustawa ECPA została dodatkowo zmieniona przez ustawę **Communications Assistance for Law Enforcement Act** (CALEA). CALEA nałożyła na dostawców usług internetowych obowiązek udostępnienia ich sieci organom ścigania w celu prowadzenia zgodnego z prawem nadzoru.

  Znajomość przepisów ECPA ma kluczowe znaczenie dla organizacji, które są obecne w Stanach Zjednoczonych. Przepisy prawa stanowią, że prowadzenie inwigilacji i przechwytywanie ruchu w sieciach, nawet kontrolowanych przez organizację, jest przestępstwem, jeśli użytkownicy mają uzasadnione oczekiwania co do prywatności. W przypadku członków zespołu CSIRT tworzy to potencjalne problemy prawne w uzyskiwaniu dostępu do zasobów sieciowych lub innych systemów. Można temu łatwo zaradzić, jeśli wszyscy użytkownicy systemu potwierdzą, że rozumieją, że ich własna komunikacja może być monitorowana przez organizację i że nie mają uzasadnionych oczekiwań co do prywatności swojej komunikacji podczas korzystania z komputerów i zasobów sieciowych zapewnianych przez organizację.
- **Economic Espionage Act of 1996** (**EEA**). Ustawa ta zawiera kilka postanowień zawartych w 18 USC § 1831 – 1839 i uznaje szpiegostwo gospodarcze oraz kradzież tajemnic handlowych za przestępstwo. Przepisy te rozszerzają poprzednie przepisy dotyczące szpiegostwa bezpośrednio na organizacje komercyjne, nie ograniczając ich do kwestii bezpieczeństwa narodowego lub informacji rządowych.

Zasady postępowania z dowodami

Federalne zasady postępowania z dowodami stanowią bazę, na podstawie której dowody mogą zostać dopuszczone w postępowaniu karnym lub cywilnym albo wykluczone z nich. Dla członków zespołu CSIRT znajomość poniższych zasad jest ważna, ponieważ stosowanie się do nich ma na celu uniknięcie zanieczyszczenia zebranych dowodów, które w konsekwencji zostałyby wyłączone z postępowania sądowego.

- **Reguła 402 — test na obecność odpowiednich dowodów**. Ta zasada składa się z dwóch części. Po pierwsze, dowód, który ma zostać dopuszczony do postępowania, musi czynić zdarzenie mniej lub bardziej prawdopodobnym, niż miałoby to miejsce bez tego dowodu. Po drugie, dowody lub fakty, na które dowody wskazują, muszę mieć znaczenie dla prowadzonego postępowania. Oznacza to, że dowody powinny być nie tylko istotne dla postępowania, ale także potwierdzać lub obalać niektóre aspekty sprawy.
- **Reguła 502 — przywilej adwokata i klienta oraz produkt pracy**. Jedną z najświętszych zasad współczesnego prawa jest relacja między klientem a jego adwokatem. Jedno z postanowień tajemnicy adwokackiej stanowi, że to, co między nimi zostanie powiedziane, nie może zostać ujawnione w sądzie. Dotyczy to nie tylko komunikacji ustnej, ale również pisemnej. W świecie kryminalistyki cyfrowej bardzo często powstają raporty dotyczące podjętych działań i uzyskanych informacji. Wielokrotnie osoby reagujące na incydenty będą bezpośrednio współpracować z prawnikami w imieniu swoich klientów. W rezultacie raporty przygotowane w związku z incydentem mogą podlegać właśnie tym zasadom. W przypadku współpracy z prawnikami zrozumienie tego jest bardzo ważne, podobnie jak zrozumienie, kiedy zasady te mogą mieć zastosowanie.
- **Reguła 702 — zeznania biegłych**. Na podstawie zdobytego doświadczenia i wiedzy w zakresie kryminalistyki cyfrowej analityk może zostać dopuszczony do składania zeznań jako biegły. Jest to reguła dowodowa określająca specyfikę zeznań biegłych.
- **Reguła 902 — dowody samouwierzytelniające się**. 1 grudnia 2017 roku reguła ta została zmieniona w odniesieniu do kryminalistyki cyfrowej. Nowo dodane przepisy dotyczą możliwości dokonywania weryfikacji integralności dowodów cyfrowych na podstawie haszowania (zostanie to omówione w kolejnych rozdziałach). Ponadto zasada ta wymaga, by dowody przedstawiała osoba wykwalifikowana oraz by zostały one zebrane zgodnie z najlepszymi praktykami.
- **Reguła 1002 — reguła najlepszego dowodu**. W postępowaniu cywilnym lub karnym oryginalne zapiski, nagrania lub zdjęcia muszą zostać przedstawione jako dowód, chyba że można zrobić uzasadniony wyjątek od tej reguły. W sferze fizycznej łatwo jest przedstawić fizyczne dowody. Strony w sprawie mogą z łatwością okazać nóż użyty podczas napadu. Staje się to nieco bardziej skomplikowane, gdy dowodem jest zapis magnetyczny na dysku twardym lub pliki dziennika pochodzące z routera. W tym przypadku sądy orzekły, że obraz dysku twardego z materiału dowodowego jest rozsądnym zamiennikiem rzeczywistego dysku twardego, który został zbadany.

- **Reguła 1003 — dopuszczalność duplikatów**. Jednym z najbardziej krytycznych kroków podczas przeprowadzania badania kryminalistycznego nośników cyfrowych jest wykonanie obrazu lub kopii kryminalistycznej nośnika. Ta reguła dowodowa pozwala na dopuszczenie takiego obrazu w sądzie. Należy zauważyć, że jeśli obraz lub kopia kryminalistyczna mają zostać dopuszczone, to analityk, który wykonał tę czynność, najprawdopodobniej będzie musiał zeznać, że zrobił to prawidłowo.

W dalszej części przyjrzymy się podstawowym procedurom kryminalistyki cyfrowej, które mają zastosowanie w reagowaniu na incydenty.

Procedury kryminalistyczne w reagowaniu na incydenty

Jak stwierdzono w poprzednim rozdziale, kryminalistyka cyfrowa jest ważnym elementem reagowania na incydenty. Często dzięki zastosowaniu cyfrowych metod kryminalistycznych osoby reagujące na incydenty mogą uzyskać jasne zrozumienie łańcucha zdarzeń, które doprowadziły do złośliwych działań, takich jak przejęcie serwera lub inne naruszenie bezpieczeństwa danych. W przypadku innych incydentów, na przykład oszustwa wewnętrznego lub złośliwego działania osób poufnych, kryminalistyka cyfrowa może również umożliwić wskazanie winnego. Przed szczegółowym omówieniem narzędzi i technik dostępnych dla osób reagujących na incydenty niezwykle ważne jest omówienie podstawowych elementów kryminalistyki cyfrowej. Stanowi to nie tylko kontekst dla konkretnych działań, ale także metodę zapewniającą przydatność dowodów uzyskanych w ramach dochodzenia w sprawie incydentu.

Krótka historia kryminalistyki cyfrowej

Organy ścigania po raz pierwszy zaczęły zwracać uwagę na rolę, jaką komputery odgrywają w działalności przestępczej, w połowie lat 80. Wcześniej istniejące przepisy i techniki egzekwowania prawa nie były skuteczne w identyfikowaniu i ściganiu przestępców komputerowych. W momencie, gdy wykorzystanie komputerów przez przestępców zaczęło zyskiwać na znaczeniu, agencje, takie jak **Federalne Biuro Śledcze** (FBI) Stanów Zjednoczonych, zdecydowały się na uwzględnienie w swojej działalności specjalnych możliwości prowadzenia dochodzeń cyfrowych i kryminalistycznych. Doprowadziło to do powstania zespołu FBI **Computer Analysis and Response Team** (CART). Inne agencje, takie jak Metropolitan Police Service, także zaczęły działać w kierunku stworzenia możliwości prowadzenia dochodzeń w sprawie cyberprzestępczości.

Zespół CART FBI

Doskonałym dokumentem historycznym odnoszącym się do CART FBI jest krótki artykuł sygnowany przez United States Department of Justice, opublikowany w „Crime Laboratory Digest" w styczniu 1992 roku: *https://www.ncjrs.gov/pdffiles1/Digitization/137561NCJRS.pdf*.

Potrzebę prowadzenia dochodzeń w cyberprzestrzeni oraz analizy kryminalistycznej uświadomiły szerokiemu gronu osób dwa doniosłe wydarzenia. Pierwszym z nich było włamanie hakera Markusa Hessa do Lawrence Berkeley National Laboratory. Mogło ono pozostać niewykryte, gdyby nie wysiłki Clifforda Stolla, który opracował plan złapania napastnika w pułapkę, by wyśledzić jego połączenie. Wysiłki te się opłaciły i Stoll wraz z innymi organami był w stanie wyśledzić hakera i ostatecznie oskarżyć go o szpiegostwo. W następnym rozdziale dogłębnie omówimy wysiłki Stolla, ponieważ oprócz istotnego kroku w rozwoju kryminalistyki cyfrowej jego techniki dochodzeniowe stanowią doskonały materiał edukacyjny.

Drugim głośnym wydarzeniem był rozprzestrzenianie się robaka Morris w dopiero co rozwijającym się internecie w 1988 roku. Robak ten, stworzony i wydany przez Roberta Tappana Morrisa, wywołał odmowę usługi na kilku tysiącach systemów, powodując szkody na ponad 100 tysięcy dolarów. Dochodzenie po incydencie przeprowadzone przez kilka osób, w tym Clifforda Stolla, wykazało, że zainfekowanych zostało co najmniej 6 tysięcy systemów. Gwałtowne rozprzestrzenianie się robaka i związane z nim szkody doprowadziły do powstania **CERT Coordination Center** (CERT/CC) przy Carnegie Mellon University.

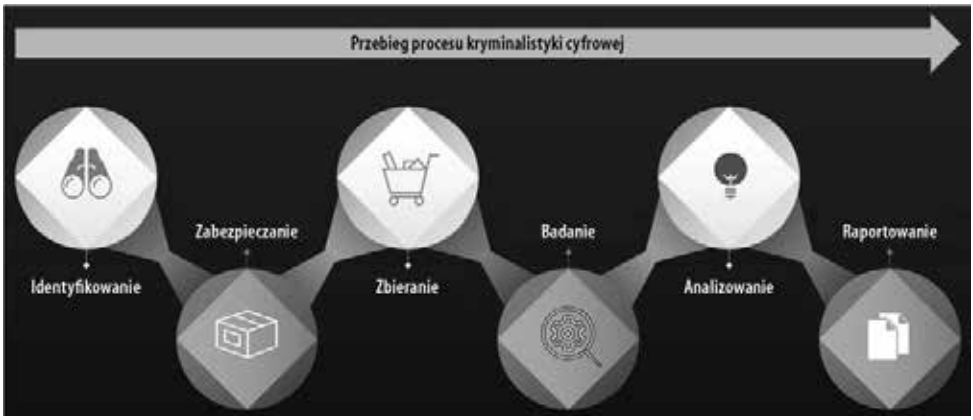
W latach 90., gdy coraz więcej organów ścigania zaczęło uwzględniać kryminalistykę cyfrową w kontekście swoich możliwości dochodzeniowych, potrzeba standaryzacji procesów kryminalistycznych stała się bardziej oczywista. W 1993 roku zorganizowano międzynarodową konferencję poświęconą roli dowodów komputerowych. Wkrótce potem, w 1995 roku, powstała organizacja **International Organization on Computer Evidence** (IOCE). Organ ten został utworzony w celu opracowania wytycznych i standardów dotyczących różnych etapów procesu cyfrowego badania kryminalistycznego. W 1998 roku we współpracy z IOCE federalni dyrektorzy laboratoriów kryminalistycznych utworzyli **Scientific Working Group on Digital Evidence** (SWGDE). Grupa ta reprezentowała amerykański wkład IOCE zmierzający do standaryzacji praktyk kryminalistycznych w dziedzinie cyfrowej.

W miarę jak organizacje kontynuowały standaryzację praktyk, organy ścigania nadal włączały kryminalistykę cyfrową do swoich ogólnych możliwości kryminalistycznych. W 2000 roku FBI utworzyło pierwsze laboratorium **Regional Computer Forensic Laboratory** (RCFL). Laboratoria te zostały utworzone w celu umożliwienia organom ścigania prowadzenia dochodzenia na różnych poziomach w różnych sprawach dotyczących cyberprzestępczości. Możliwości RCFL znacznie wzrosły w ciągu ostatnich dwóch dekad i powstało 17 różnych laboratoriów RCFL rozsianych po całych Stanach Zjednoczonych. Ponadto inne federalne, stanowe i lokalne agencje policyjne utworzyły liczne cyfrowe jednostki śledcze. Przy stale rosnącej liczbie przypadków przestępstw związanych z komputerami agencje te ciągle wykonują swoją niezwykle istotną pracę.

Proces kryminalistyki cyfrowej

Podobnie jak proces reagowania na incydenty, proces kryminalistyki cyfrowej definiuje przepływ dowodów cyfrowych związanych z incydentem od momentu jego pierwszej identyfikacji do momentu przedstawienia go kierownictwu wyższego szczebla lub organowi ścigania, takiemu jak sąd. Istnieje kilka schematów, które definiują ten proces

i w większości przebiega on na nich podobną ścieżką. W tym przypadku będziemy wykorzystywać ramy prowadzenia dochodzeń cyfrowych **Digital Forensics Research Workshop** (DFRWS). Struktura ta została przedstawiona na rysunku 3.1.



Rysunek 3.1. Przebieg procesu kryminalistyki cyfrowej

Ramy obejmują sześć elementów:

- identyfikowanie,
- zabezpieczanie,
- zbieranie,
- badanie,
- analizowanie,
- raportowanie.

Z punktu widzenia reagowania na incydenty w normalnej sytuacji personel nie będzie przejmował elementów sieci ani krytycznych systemów i wyłączał ich, chyba że zaistnieje ku temu ważny powód. Jest to jedno z działań równoważących nieodłącznie związanych z kryminalistyką cyfrową i reagowaniem na incydenty. Całkowicie cyfrowe podejście kryminalistyczne polega na zebraniu wszystkich istotnych dowodów, zabezpieczeniu ich i przetworzeniu.

Ten proces może wymagać miesięcy pracy, w zależności od rodzaju incydentu. Takie podejście, choć dokładne i szczegółowe, może na pewien czas pozbawić organizację krytycznych komponentów. Po miesięcznej analizie zespół CSIRT może być w stanie przekazać kierownictwu, który łańcuch zdarzeń doprowadził do naruszenia, jednak będzie to bezcelowe, gdyby utracony został cały miesięczny przychód.

Badacze przydzieleni do zespołu CSIRT muszą być gotowi do zrównoważenia potrzeby uzyskania wymaganej dokładności z potrzebą wznowienia lub kontynuowania normalnej działalności organizacji.

Identyfikowanie

Proces kryminalistyki cyfrowej rozpoczyna się od identyfikacji potencjalnych dowodów. W tym miejscu wchodzi w grę omówiona wcześniej zasada wymiany Lockarda. Zasada ta może zostać wykorzystana do identyfikacji potencjalnych źródeł dowodów podczas incydentu. Na przykład jeśli zespół CSIRT będzie próbował określić pierwotną przyczynę infekcji złośliwym oprogramowaniem w systemie, to zacznie od analizy zainfekowanego systemu. Ponieważ niektóre złośliwe programy wymagają dostępu do serwera C2, analitycy mogą przeanalizować połączenia zapory sieciowej lub dzienniki proxy pod kątem ruchu wychodzącego z zainfekowanego systemu na zewnętrzne adresy IP. Zbadanie adresów IP tych połączeń może doprowadzić do ujawnienia serwera C2 i potencjalnie do uzyskania bardziej szczegółowych informacji na temat konkretnego wariantu złośliwego oprogramowania, które zainfekowało system.

Należy jednak zauważyć, że cyberprzestępcy mogą bardzo łatwo manipulować dowodami cyfrowymi, zatem poleganie na pojedynczym dowodzie cyfrowym bez innych dowodów potwierdzających należy zawsze traktować z ostrożnością. Dowód należy zweryfikować, zanim będzie można mu zaufać.

Zabezpieczanie

Po zidentyfikowaniu dowodów ważne jest, by zabezpieczyć je przed wszelkimi modyfikacjami lub usunięciem. W przypadku dowodów takich jak pliki dziennika konieczne może okazać się włączenie kontroli chroniących pliki dziennika przed usunięciem lub modyfikacją. Jeśli chodzi o systemy hostów, takie jak komputery stacjonarne, to może okazać się konieczne odizolowanie systemu od reszty sieci za pomocą kontroli fizycznych lub logicznych, kontroli dostępu do sieci lub kontroli obwodowej. Bardzo ważne jest również, by żaden użytkownik nie miał dostępu do podejrzanego systemu. Gwarantuje to, że użytkownicy celowo lub nieumyślnie nie zanieczyszczą dowodów. Inny aspekt zabezpieczania jest związany ze zwiększoną zależnością od platform wirtualnych. Zachowanie tych systemów można osiągnąć za pomocą systemów tworzenia migawek i zapisywania maszyn wirtualnych w nieulotnej pamięci masowej.

Zbieranie

Etap zbierania dowodów to punkt, w którym badacze zajmujący się kryminalistyką cyfrową rozpoczynają proces pozyskiwania dowodów cyfrowych. Podczas badania dowodów cyfrowych ważne jest, by zrozumieć niestabilny charakter niektórych dowodów. Dowody nietrwałe to takie, które mogą zostać utracone, gdy system zostanie wyłączony. W przypadku sprzętu sieciowego może to obejmować aktywne połączenia lub dane dziennika przechowywane na urządzeniu. W przypadku laptopów i komputerów stacjonarnych dane ulotne obejmują pamięć operacyjną lub pamięć podręczną protokołu ARP (**Address Resolution Protocol**).

Zespół **Internet Engineering Task Force** (IETF) opracował dokument zatytułowany *Guidelines for Evidence Collection and Archiving (RFC 3227)*, który określa stopień ulotności dowodów cyfrowych w następujący sposób:

- rejestry i pamięć podręczna,
- tabela routingu, pamięć podręczna ARP, tabela procesów, statystyki jądra, pamięć (RAM),
- systemy plików tymczasowych,
- obrazy dysków,
- zdalne rejestrowanie i monitorowanie konfiguracji danych fizycznych, topologia sieci,
- nośniki archiwalne.

Badacze zajmujący się kryminalistyką cyfrową muszą koniecznie uwzględnić tę ulotność w swoim procesie zbierania dowodów. Należy zastosować odpowiednie metody, dzięki którym dowody ulotne zostaną zgromadzone i przeniesione na nieulotne nośniki, takie jak zewnętrzny dysk twardy.

Właściwe postępowanie z dowodami

Właściwe obchodzenie się z dowodami i ich odpowiednie zabezpieczenie mają kluczowe znaczenie. Błędy popełnione podczas pozyskiwania dowodów mogą doprowadzić do ich sfałszowania, a następnie do braku rzetelności kryminalistycznej. Ponadto, jeśli incydent wiąże się z potencjalnymi kwestiami prawnymi, to krytyczne dowody mogą zostać niedopuszczone do postępowania karnego lub cywilnego. Istnieje kilka kluczowych zasad postępowania z dowodami, których to zasad należy przestrzegać:

- **Modyfikowanie oryginalnych dowodów**. Działania podjęte przez ekspertów kryminalistyki cyfrowej nie powinny zmieniać oryginalnych dowodów. Na przykład analitycy kryminalistyczni nie powinni uzyskiwać dostępu do działającego systemu, jeśli nie jest to konieczne. Należy zauważyć, że pewne aktywności mogą potencjalnie zmienić niektóre dowody. Włączając odpowiednią dokumentację oraz przedstawiając uzasadniony powód, eksperci kryminalistyczni mogą zredukować prawdopodobieństwo uznania dowodów za sfałszowane.
- **Dokumentowanie**. Jednym z częstych stwierdzeń przedstawicieli organów ścigania jest zdanie: *jeśli tego nie zapisałeś, to się nie wydarzyło*. Jest to szczególnie prawdziwe w przypadku kryminalistyki cyfrowej. Każde podjęte działanie powinno zostać udokumentowane w taki czy inny sposób. Dotyczy to sporządzania szczegółowych notatek i schematów. Innym sposobem dokumentowania są zdjęcia. Właściwa dokumentacja pozwala ekspertom na odtworzenie łańcucha zdarzeń, jeśli kiedykolwiek zakwestionowana zostanie integralność dowodów.

Wytyczne postępowania z dowodami

Różne organy ścigania dysponują szeroką gamą zasobów dotyczących właściwego postępowania z dowodami w terenie. Zalecane jest zapoznanie się z tymi procedurami. Wykorzystywane przez organy ścigania są następujące przewodniki:

- *http://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf*,
- *https://www.ncjrs.gov/pdffiles1/nij/219941.pdf*,
- *https://www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf*.

Łańcuch dozoru

Łańcuch dozoru opisuje dokumentację dowodu w całym jego cyklu życia. Ten cykl życia rozpoczyna się, gdy dana osoba po raz pierwszy przejmuje kontrolę nad dowodem, a kończy się, gdy incydent zostanie ostatecznie zakończony, a dowód może zostać zwrócony lub zniszczony. Utrzymanie odpowiedniego łańcucha dozoru ma kluczowe znaczenie. W przypadku konieczności wniesienia dowodu na salę sądową każde zerwanie łańcucha dozoru może skutkować wykluczeniem dowodu z postępowania. Z tego powodu niezwykle ważne jest, by rejestrować cały cykl życia dowodu.

Zespół CSIRT może rejestrować i utrzymywać łańcuch dozoru na dwa podstawowe sposoby.

Pierwszą metodą jest rejestracja **elektroniczna**. Istnieją producenci, którzy dostarczają organizacjom, takim jak laboratoria kryminalistyczne lub organy ścigania, sprzęt i oprogramowanie automatyzujące proces kontroli łańcucha dozoru. Systemy te wykorzystują naklejki z kodami kreskowymi unikatowe dla każdego dowodu. Podczas skanowania tych kodów tworzony jest ślad elektroniczny.

Drugą metodą tworzenia i utrzymywania łańcucha dozoru jest metoda **papieru i długopisu**. Wykorzystuje papierowe formularze, które zawierają informacje niezbędne do rozpoczęcia i utrzymania łańcucha. Pomimo że metoda taka może być nieco kłopotliwa i wymagać większej staranności w celu zabezpieczenia formularza przed zniszczeniem lub zmanipulowaniem, jest to znacznie bardziej opłacalne rozwiązanie dla mniejszych zespołów CSIRT, które mogą nie dysponować zasobami niezbędnymi do wdrożenia rozwiązania zautomatyzowanego.

W formularzu łańcucha dozoru konieczne jest podanie szczegółowych informacji dla kilku sekcji. Szablon formularza łańcucha dozoru został przedstawiony na rysunku 3.2. Edytowalny formularz łańcucha dozoru jest dostępny w NIST pod adresem *https://www.nist.gov/document/sample-chain-custody-formdocx*.

Pierwszą sekcją, którą należy wypełnić, jest sekcja *Incident Information* (informacje o zdarzeniu), którą pokazano na rysunku 3.3. Pole *Intake ID* (identyfikator) wymaga podania unikatowego identyfikatora sprawy lub incydentu. Może to być numer zdarzenia lub numer systemu biletowego. Drugie pole, *Analyst* (analityk), określa analityka wypełniającego pierwsze sekcje formularza łańcucha dozoru. Wreszcie, każdy oddzielny element dowodowy wymaga numeru *Submission* (przedłożenia). Zapewnia to, że każdy dowód będzie miał swój własny, oddzielny formularz łańcucha dozoru.

Druga z tych sekcji to szczegółowy opis przedmiotu. Uwzględnienie kilku dodatkowych elementów może wydawać się zbędne, jednak kryminalistyka cyfrowa polega na utrzymaniu szczegółowości. Zarejestrowanie informacji nie pozostawia wątpliwości co do ich autentyczności. Opis ten powinien zawierać następujące elementy:

- *Item number* (numer przedmiotu). Na formularzu należy podać unikatowy numer przedmiotu. Jeśli istnieje wiele elementów dowodu, to wypełniony powinien zostać oddzielny formularz łańcucha dozoru.
- *Description* (opis). Jest to ogólny opis przedmiotu. Może to być proste stwierdzenie, na przykład „dysk twardy SATA 500 GB”.
- *Manufacturer* (producent). Ten szczegół jest pomocny, gdy dostępnych jest wiele dowodów, które mogą pochodzić od różnych producentów.

IR PROACTIVE

Computer Security Incident Response Chain of Custody Form

Incident Information

Intake ID:	Analyst	Submission #:

Electronic Media Details

Item Number:	Description:	
Manufacturer:	Model:	Serial Number:

Image or File Details

Date / Time Acquired:	Created By:	Method:	Image Drive:
File Image Name:		Hash:	

Chain of Custody

Tracking No:	Date/Time:	FROM:	TO:	Reason:
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	
	Date:	Name/Org:	Name/Org:	
	Time:	Signature:	Signature:	

Page of

IRProactive-DFIR-01 v 1.0 March 6, 2022

Rysunek 3.2. Formularz łańcucha dozoru dowodu

Incident Information

Intake ID: 2022-00056	Analyst Johansen, G	Submission #: 001

Rysunek 3.3. Sekcja informacji o zdarzeniu w formularzu łańcucha dozoru

- *Model* (model). Ze względu na to, że istnieć może wiele różnych numerów modeli danego komponentu, zapisanie ich zapewnia dalsze szczegółowe informacje o przedmiocie.
- *Serial Number* (numer seryjny). Ma to krytyczne znaczenie w przypadku, gdy incydent dotyczy kilku systemów o dokładnie takiej samej konfiguracji. Wyobraźmy sobie, jak wyglądałaby próba zrekonstruowania, który łańcuch dozoru jest powiązany z którym dyskiem twardym, w przypadku gdyby skonfiskowanych zostało sześć dysków tej samej marki i o tym samym numerze modelu.

Wypełniona sekcja szczegółów mediów elektronicznych może wyglądać tak jak na rysunku 3.4.

Electronic Media Details

Item Number:	Description:	
001	'easystore' External HDD	
Manufacturer:	Model#	Serial Number:
Western Digital	1621B	WX62D80FVXN1

Rysunek 3.4. Sekcja szczegółów mediów elektronicznych w formularzu łańcucha dozoru

Sekcji alternatywnej można użyć w okolicznościach, w których dowodem może być plik logiczny, taki jak pliki dziennika lub obrazy zarejestrowane podczas dochodzenia. Należą do niej następujące elementy:

- *Date/Time Acquired* (data/godzina pozyskania). Ważne jest dokładne określenie daty i godziny pozyskania określonych plików.
- *Description* (opis). Krótki opis pozyskanych mediów, który może być przydatny. Jeśli do pozyskania dowodów wykorzystywana jest aplikacja lub narzędzie kryminalistyczne, należy to odnotować. W innych okolicznościach, na przykład w przypadku plików dziennika, może to być po prostu kopia zewnętrznego dysku twardego.
- *Storage Drive* (dysk pamięci masowej). W dalszej części omówimy istotność posiadania zewnętrznych nośników do przechowywania plików. W formularzu należy odnotować, jaki dokładnie zastosowany został napęd dyskowy.
- *File/Image Name* (nazwa pliku/obrazu). W tym miejscu wstawiana jest unikatowa nazwa pliku lub obrazu.
- *Hash*. Dla każdego pozyskanego pliku należy obliczyć unikatową wartość hash.

Wypełniona sekcja *Image or File Details* (szczegóły obrazu lub pliku) w formularzu łańcucha dozoru powinna wyglądać jak na rysunku 3.5.

Image or File Details

Date / Time Acquired:	Created By:	Method:	Storage Drive:
March 15, 2022, 0113 UTC	Johansen, G	TCPDump	Forensics HDD-01
File/Image Name:		Hash:	
CoreRouter.pcap		f1e815e58c168ac377b8cf576bd1db68	

Rysunek 3.5. Sekcja szczegółów obrazu lub pliku w formularzu łańcucha dozoru

Kolejna sekcja zawiera wyszczególnione etapy, przez które przeszedł dowód w swoim cyklu życia. Dla każdego etapu należy uchwycić następujące szczegóły:

- *Tracking No* (numer śledzenia). Jest to numer wskazujący etap cyklu życia, przez który przeszedł dowód.
- *Date/Time* (data/godzina). Jest to kluczowa informacja w każdym łańcuchu dozoru i dotyczy w równym stopniu każdego etapu, przez który przeszedł dowód. Dzięki temu każda osoba analizująca łańcuch dozoru może zrekonstruować, z dokładnością do minuty, każdy krok w cyklu życia łańcucha dozoru.

- *FROM/TO* (OD/DO). Pola te mogą oznaczać osobę lub miejsce przechowywania. Na przykład jeśli analityk przechwycił dysk twardy i obecnie transportuje go do bezpiecznego schowka, zostanie to odnotowane jako lokalizacja *DO*. Bardzo ważne jest, by osoby wymienione w łańcuchu dozoru podpisały formularz, gdy ma to zastosowanie w celu wyegzekwowania odpowiedzialności.
- *Reason* (powód). Nigdy nie należy przenosić dowodu bez powodu. Jeśli tak się zdarzy, to w tej części formularza można określić przyczynę.

Na rysunku 3.6 przedstawiony został przykład przeniesienia dysku twardego zarejestrowanego na rysunku 3.5. Przemieszczenie każdego pojedynczego dowodu jest w tym przypadku rejestrowane. Pierwszym krokiem jest faktyczne zajęcie dysku z systemu. W tym przypadku nie ma indywidualnego opiekuna, ponieważ dysk został pobrany z centrum danych. Istotne jest to, że autor jest osobą przejmującą dysk, aż do momentu przekazania go do Carol Davis z IRProactive w celu wykonania analizy.

Chain of Custody

Tracking No:	Date/Time	FROM:	TO:	Reason:
1	Date: 03/15/22	Name/Org: Gerard Johansen IRProactive	Name/Org: Carol Davis IRProactive Evidence Custodian	Evidence acquisition and storage
	Time:0126 UTC	Signature: Gerard Johansen	Signature: Carlos Davis	
2	Date: 03/16/22	Name/Org: Carol Davis	Name/Org: Gerard Johansen	Analysis
	Time: 1642 UTC	Signature: Carlos Davis	Signature: Gerard Johansen	

Rysunek 3.6. Szczegóły łańcucha dozoru

Łańcuch dozoru jest utrzymywany przez cały okres istnienia dowodu. Nawet jeśli dowody zostaną zniszczone lub zwrócone, to w formularzu łańcucha dozoru dokonuje się odpowiedniego wpisu. Formularze te należy przechowywać wraz z wszelkimi innymi materiałami wygenerowanymi w wyniku incydentu, co powinno stanowić część każdego kolejnego tworzonego raportu.

Badanie

Faza badania polega na wyszczególnieniu konkretnych narzędzi i technik kryminalistycznych, które będą wykorzystywane do wykrywania i wydobywania danych z dowodów zajętych podczas incydentu. Na przykład w przypadku, gdyby istniało podejrzenie, że złośliwe oprogramowanie zainfekowało komputer stacjonarny w ramach większego ataku, wówczas na tym etapie miałoby miejsce wyodrębnienie określonych informacji z pozyskanego obrazu pamięci. W innych przypadkach personel odpowiedzialny za przeprowadzenie kryminalistyki cyfrowej może potrzebować wyodrębnionego ruchu **Secure Shell** (SSH) z przechwytywania sieci. Badanie cyfrowego materiału dowodowego jest również kontynuacją procesu właściwego przechowywania i polega na zachowaniu dowodu z najwyższą starannością podczas badania. Jeśli ekspert kryminalistyki cyfrowej nie zadba o zachowanie dowodów na tym etapie, istnieje możliwość zanieczyszczenia, co spowodowałoby, że dowody stałyby się niewiarygodne lub bezużyteczne.

Analizowanie

Po wydobyciu potencjalnie istotnych fragmentów danych w fazie badania ekspert kryminalistyki musi dokonać analizy danych, uwzględniając wszelkie inne uzyskane istotne dane. Na przykład jeśli analityk kryminalistyki cyfrowej wykryje, że zagrożony host ma otwarte połączenie z zewnętrznym adresem IP, to skojarzy tę informację z analizą pakietów przechwyconych z sieci. Używając adresu IP jako punktu wyjścia, analityk mógłby wyizolować ten ruch. Następnie analityk może być w stanie ustalić, że zagrożony host wysyła sygnał nawigacyjny do serwera C2. Stąd, korzystając z dodatkowych źródeł, analityk może być w stanie określić, który wektor ataku jest powiązany z tym adresem IP.

Raportowanie

Raportowanie faktów związanych z kryminalistyką cyfrową musi być jasne, zwięzłe i bezstronne. Niemal we wszystkich przypadkach biegły sądowy będzie musiał przygotować szczegółowy pisemny raport, który będzie dotyczył każdego działania i zawierał wymagane krytyczne dane. Ten raport powinien być kompletny, dokładny i niestronniczy. Bardzo często dokument taki stanowi część większego dochodzenia w sprawie incydentu i jest pomocny w ustaleniu jego pierwotnej przyczyny.

Innym aspektem raportowania jest rola, jaką biegły sądowy może pełnić w postępowaniu karnym lub cywilnym. Jeśli incydent będący przedmiotem dochodzenia ujawnił podejrzanego lub inną osobę odpowiedzialną, to dodatkowo wymagane może być złożenie zeznań w sądzie. To właśnie podczas tego zeznania biegły sądowy będzie musiał przedstawić fakty z badania kryminalistycznego, w mniej więcej taki sam beznamiętny sposób jak w raporcie. Badacz będzie musiał zaprezentować dokonania i wnioski bez uprzedzeń i może być ograniczony w zakresie wydawanych przez siebie opinii. To, w jaki sposób badacz będzie mógł zeznawać, często zależy od jego przeszkolenia i doświadczenia. Niektórzy mogą zostać ograniczeni jedynie do przedstawienia faktów wynikających z przeprowadzonego badania. Gdy ekspert jest już doświadczony i zostanie uznany za biegłego sądowego, może być w stanie wydać własną opinię.

Laboratorium kryminalistyki cyfrowej

Działania w zakresie kryminalistyki cyfrowej to proces wymagający, w którym należy wykorzystać odpowiednie narzędzia, techniki i wiedzę w celu wydobycia potencjalnych dowodów z systemów. Bardzo istotną sprawą jest zapewnienie, by miejsce pracy ekspertów kryminalistycznych było inne niż miejsce prowadzenie normalnej działalności biznesowej organizacji. Najłatwiej jest to osiągnąć poprzez zapewnienie członkom CSIRT bezpośrednio zaangażowanym w badanie dowodów cyfrowych lokalizacji całkowicie oddzielonej od reszty organizacji. Cyfrowe laboratorium kryminalistyczne powinno mieć kilka kluczowych cech, tak by zapewnić badaczom niezbędną prywatność, ale także zapewnić integralność dowodów podczas ich badania.

Bezpieczeństwo fizyczne

Dostęp do laboratorium kryminalistycznego musi być ściśle kontrolowany. W celu zachowania łańcucha dozoru dostęp do laboratorium powinien mieć tylko ten personel, który ma taką uzasadnioną potrzebę. Ograniczenie to jest konieczne w celu wyeliminowania

wszelkich możliwości sfałszowania lub zniszczenia dowodów. Z tego powodu laboratorium powinno być przez cały czas zamknięte. W idealnej sytuacji dostęp powinien być udzielany za pomocą kart dostępu lub breloków, z centralnym systemem zarządzania dostępem. Umożliwia to pełną rekonstrukcję ruchu całego personelu w laboratorium w określonym czasie.

W laboratorium powinny również znajdować się szafki na dowody umożliwiające ich odpowiednie przechowywanie, gdy nie są badane. Szafki powinny być zabezpieczone za pomocą zamka lub zamka szyfrowego. Klucze do tych szafek powinny być zabezpieczone w laboratorium, a dostęp do nich powinni mieć wyłącznie badacze. Jeśli organizacja dysponuje odpowiednimi zasobami, to każdy konkretny incydent powinien mieć własną szafkę, a wszystkie dowody powinny znajdować się w jednej szafce. Zmniejsza to ryzyko pomieszania dowodów cyfrowych.

Klimat i wilgotność powinny być kontrolowane w taki sam sposób, jak w każdym centrum danych, a parametry te powinny być ustawione na odpowiednich poziomach.

Narzędzia

W zależności od konkretnych badań, które mają zostać przeprowadzone, konieczne może okazać się wykonanie pewnych prac, takich jak wykręcenie śrub lub przecięcie przewodów. Z tego powodu badacze powinni mieć do dyspozycji podręczny zestaw narzędzi. Laboratorium powinno być również zaopatrzone w pudełka do zabezpieczania dowodów. Jeśli jednym z zadań badaczy ma być sprawdzenie smartfonów lub tabletów, to powinni mieć zapewnione klatki Faradaya. Torby te umożliwiają egzaminatorom odizolowanie smartfonu lub tabletu od sieci komórkowej przy jednoczesnym utrzymaniu źródła zasilania.

Sprzęt komputerowy

Laboratorium powinno być wyposażone w wystarczającą liczbę komputerów i innego sprzętu do wykonywania różnych niezbędnych działań. Zadaniem egzaminatorów może być tworzenie obrazów dysków twardych i przetwarzanie gigabajtów danych. W rezultacie niezbędny jest komputer kryminalistyczny z wystarczającą ilością pamięci RAM. Pomimo że istnieją osobiste preferencje dotyczące ilości pamięci RAM, to zalecane jest minimum 32 GB tej pamięci. Badacze często pracują z dużą ilością danych. W konsekwencji, oprócz pamięci i mocy obliczeniowej, kryminalistyczne stacje robocze powinny mieć główny dysk na system operacyjny, który może zawierać oprogramowanie kryminalistyczne, oraz dodatkowy dysk do przechowywania dowodów. Dysk dodatkowy powinien oferować co najmniej 2 TB przestrzeni dyskowej.

Oprócz stacji roboczej badacze powinni mieć również do dyspozycji komputery z dostępem do internetu. Sama stacja robocza w celu zachowania bezpieczeństwa, a także w celu zapewnienia ochrony przed możliwym uszkodzeniem dowodów podczas badania kryminalistycznego nie powinna mieć połączenia z internetem. Do prowadzenia badań lub pisania raportów wykorzystywany powinien być inny, dodatkowy komputer.

Kolejnym istotnym urządzeniem jest fizyczna blokada zapisu. To urządzenie pozwala na połączenie między dyskiem twardym zajętym jako dowód a maszyną do obrazowania kryminalistycznego. Podstawowa różnica między tą fizyczną blokadą zapisu a połączeniem

USB lub Thunderbolt polega na tym, że ekspert kryminalistyki może mieć pewność, że na dysku dowodowym nie zostaną zapisane żadne dane. Rysunek 3.7 przedstawia blokadę fizycznego zapisu Tableau eSATA Forensic Bridge.

Rysunek 3.7. Fizyczna blokada zapisu

W przypadku cyfrowych laboratoriów kryminalistycznych, które wykonują większą liczbę zadań obrazowania, istnieje możliwość włączenia dedykowanej stacji obrazowania kryminalistycznego. Pozwala to na szybsze obrazowanie dysków dowodowych i nie angażuje stacji roboczej wykorzystywanej do badań kryminalistycznych. Wadą tego rozwiązania jest jego koszt: jeśli członkowie zespołu CSIRT nie odnotują spadku wydajności bez takiej dodatkowej stacji, to trudno może być uzasadnić taki wydatek.

Zespół CSIRT powinien również zainwestować w dyski zewnętrzne USB o dużej pojemności. Są one znacznie łatwiejsze w obsłudze i użyciu w procesie przetwarzania obrazu niż tradycyjne dyski SATA lub IDE. Dyski te mogą być wykorzystywane do przechowywania obrazu dysku dowodowego do dalszej analizy. Członkowie zespołu CSIRT powinni mieć do dyspozycji co najmniej sześć takich dysków o dużej pojemności. Na dyskach o pojemności od 2 TB do 3 TB można przechowywać kilka obrazów jednocześnie. Mniejsze dyski USB są również przydatne do przechwytywania plików dziennika i obrazów pamięci w celu późniejszego przetwarzania. Dobrym rozwiązaniem jest posiadanie dysków USB obsługujących najnowszą wersję 3.0, co umożliwia szybsze przetwarzanie.

Badacze zajmujący się kryminalistyką cyfrową, którzy wspierają zespół CSIRT, powinni mieć również do dyspozycji solidną walizkę do transportu całego niezbędnego sprzętu na wypadek konieczności przeprowadzenia badań poza siedzibą firmy. Dużo tych narzędzi jest delikatnych i wiele z nich mogłoby na przykład nie wytrzymać rzucania bagażem przez pracowników obsługi na lokalnym lotnisku. Zespół CSIRT powinien zainwestować w co

najmniej dwie twarde walizki, podobne do tych, które są używane do transportu sprzętu elektronicznego lub fotograficznego. W jednej walizce można transportować sprzęt, taki jak zewnętrzne dyski twarde, natomiast w drugiej — laptopy do analizy kryminalistycznej i minimalizować tym samym potencjalne szkody spowodowane nieostrożnym obchodzeniem się z bagażami.

Oprogramowanie

Obecnie na rynku komercyjnym i darmowym dostępnych jest wiele narzędzi programowych. Cyfrowe laboratorium kryminalistyczne powinno mieć dostęp do kilku narzędzi przeznaczonych do wykonywania podobnych działań. Jako minimum laboratorium powinno mieć oprogramowanie, które umożliwia wykonywanie obrazowania dysków dowodowych, badanie obrazów, analizowanie przechwytywanej pamięci i raportowanie wyników.

Istnieje kilka różnych rodzajów oprogramowania kryminalistycznego, z którego może korzystać analityk kryminalistyczny. Pierwszym z nich są aplikacje kryminalistyczne. Zostały specjalnie zaprojektowane do wykonywania różnorodnych zadań z zakresu kryminalistyki cyfrowej. Często są dostępne na rynku i szeroko stosowane przez organy ścigania i w społecznościach rządowych, a także w przemyśle prywatnym. Bardzo popularne i szeroko stosowane są cztery aplikacje kryminalistyczne:

- **Autopsy**. Jest to oprogramowanie open source opracowane przez Briana Carriera, które oferuje bogatą liczbę funkcjonalności do automatyzowania kluczowych zadań kryminalistyki cyfrowej. Jako projekt open source Autopsy ma również moduły open source, które zapewniają wiele dodatkowych funkcji. Program został omówiony bardziej szczegółowo w kolejnych rozdziałach.
- **EnCase**. Opracowana przez firmę OpenText aplikacja EnCase to aplikacja kryminalistyczna o pełnym spektrum działania, która wykonuje całą gamę zadań związanych z badaniem dowodów cyfrowych, pochodzących głównie z dysków twardych i innych nośników danych. Oprócz analizowania dowodów cyfrowych EnCase oferuje funkcję raportowania, która pozwala ekspertom na generowanie raportów z prowadzonej sprawy w czytelnym formacie. EnCase jest szeroko stosowany przez organy rządowe i organy ścigania. Jedyną wadą jest koszt aplikacji. Niektóre zespoły CSIRT i biegli sądowi, dysponujący ograniczonym budżetem, będą mieli problem z uzasadnieniem poniesienia tak wysokiego kosztu.
- **Forensic Toolkit** (FTK). Jest to kolejna kompleksowa aplikacja kryminalistyczna, szeroko stosowana przez organy rządowe i organy ścigania. Ma bardzo podobną funkcjonalność co EnCase, zatem oprogramowanie to może stanowić alternatywę do rozważenia przez analityków kryminalistyki cyfrowej o ograniczonym budżecie.
- **X-Ways Forensics**. Kolejną opcją jest aplikacja X-Ways Forensics. Dzięki funkcjonalności zbliżonej do aplikacji FTK i EnCase jest to doskonała, tańsza opcja skierowana do tych zespołów CSIRT, które nie potrzebują takich funkcji jak dostęp do sieci czy zdalne przechwytywanie.

Korzystaj ze sprawdzonych narzędzi

Istnieje kilka głośnych przypadków, w których zakwestionowano cyfrowe narzędzia kryminalistyczne. W Stanach Zjednoczonych prowadzony był proces Casey Anthony, sądzonej za zabójstwo swojej córki. Podczas tego procesu prokuratura przedstawiła jako dowód historię przeglądarki internetowej Anthony. Historia została wyodrębniona za pomocą narzędzia CacheBack. Recenzja tego oprogramowania przeprowadzona przez autora narzędzia wykazała, że zawierało ono błąd oprogramowania. Niewiele jest dowodów na to, że narzędzie miało wpływ na obrady ławy przysięgłych. Jest to jednak dobry przykład na to, że należy się upewnić, że narzędzia stosowane w kryminalistyce cyfrowej, szczególnie w sprawach wchodzących na drogę sądową, zostały zweryfikowane.

Narzędzia kryminalistyczne systemu operacyjnego Linux

Dostępna jest również szeroka gama dystrybucji Linuksa, które zostały stworzone na potrzeby kryminalistyki cyfrowej. Dystrybucje te są często udostępniane bezpłatnie i oferują narzędzia, które mogą pomóc śledczym zajmującym się prowadzeniem dochodzeń z zakresu cyberbezpieczeństwa. Narzędzia te można podzielić na dwa główne typy. Pierwszym z nich są dystrybucje pomyślane jako rozruchowe płyty CD/DVD lub nośniki USB. Są one przydatne do przeprowadzania segregacji lub uzyskiwania dostępu do plików bez konieczności tworzenia obrazu dysku. Dystrybucje te można umieścić na płycie CD/DVD lub, co częstsze w dzisiejszych czasach, na nośniku USB. Następnie badacz może uruchomić badany system w dystrybucji Linuksa. Dostępnych jest wiele takich dystrybucji.

Dwie najpopularniejsze wśród badaczy kryminalistyki cyfrowej dystrybucje to:

- **Digital Evidence and Forensic Toolkit (DEFT) Zero**. Dystrybucja oparta na platformie GNU Linux. DEFT można uruchomić z USB lub CD/DVD. Po uruchomieniu platforma DEFT oferuje szeroką gamę narzędzi, które mogą być wykorzystywane przez eksperta do spraw kryminalistyki cyfrowej w celu wykonywania takich działań jak odzyskiwanie pamięci masowej. Na przykład możliwe jest uzyskanie dostępu do dysku twardego w systemie, z którego jest uruchamiany. DEFT minimalizuje ryzyko dokonania zmian danych w systemie, nie uruchamiając partycji wymiany i nie używając automatycznych skryptów montowania, co zapewnia integralność pamięci systemowej. Wygląd pulpitu systemu DEFT OS został przedstawiony na rysunku 3.8.
- **Computer Aided INvestigative Environment (CAINE)**. Jest to kolejna kryminalistyczna dystrybucja Linuxa, która została wykorzystana w tej książce. CAINE to platforma GNU/Linux, która zawiera kilka narzędzi pomocnych ekspertom zajmującym się kryminalistyką cyfrową. Wygląd pulpitu systemu CAINE został przedstawiony na rysunku 3.9.

Inną kategorią dystrybucji Linuksa są dystrybucje zaprojektowane jako platformy do przeprowadzania analiz dowodów, takich jak przechwytywanie pamięci RAM i analizy dowodów sieciowych. Dostępnych jest kilka dystrybucji tego rodzaju:

- **SANS Investigative Forensic Toolkit (SIFT)**. Jest to kompleksowy zestaw narzędzi kryminalistycznych oparty na podstawowym systemie operacyjnym Ubuntu 20.04. Dołączone zostały narzędzia do obrazowania, analizy pamięci,

Rysunek 3.8. System operacyjny DEFT przeznaczony na potrzeby kryminalistyki cyfrowej

Rysunek 3.9. System operacyjny CAINE przeznaczony na potrzeby kryminalistyki cyfrowej

tworzenia osi czasu i wykonywania wielu innych zadań związanych z kryminalistyką cyfrową. SIFT jest udostępniany bezpłatnie pod adresem *https://www.sans.org/tools/sift-workstation* przez SANS Institute jako samodzielna maszyna wirtualna, plik ISO lub jako część podsystemu Windows dla systemu Linux. Po zainstalowaniu dostępny jest system oparty na dystrybucji Ubuntu, z dodatkowymi narzędziami, które są uruchamiane z wiersza poleceń lub przez GUI, jak na rysunku 3.10.

Rysunek 3.10. Stacja robocza SANS SIFT

- **CSI Linux**. Jest to kolejna bogata w funkcje platforma kryminalistyczna w CSI Linux (rysunek 3.11). Ten kryminalistyczny system operacyjny obejmuje 175 narzędzi do wykonywania różnorodnych zadań. Narzędzie jest dostępne na stronie *https://csilinux.com* jako wstępnie skonfigurowany system wirtualny, a także jako wersja bootowalna, którą można uruchomić z nośnika USB.

Rysunek 3.11. System operacyjny CSI Linux przeznaczony na potrzeby kryminalistyki cyfrowej

- **REMnux**. REMnux to wyspecjalizowane narzędzie, które łączy różne narzędzia inżynierii wstecznej złośliwego oprogramowania w zestaw narzędzi bazujący na systemie Ubuntu Linux. Niektóre z narzędzi dostępnych w REMnux zostały stworzone do analizy złośliwego oprogramowania dla systemów Windows i Linux oraz do badania podejrzanych dokumentów, a także do przechwytywania

potencjalnie szkodliwego ruchu sieciowego w odizolowanym kontenerze. Wygląd systemu REMnux został przedstawiony na rysunku 3.12.

Rysunek 3.12. System operacyjny REMNUX przeznaczony na potrzeby kryminalistyki cyfrowej

Zestawy przenośne

Jednym z aspektów reagowania na incydenty, który może stanowić wyzwanie dla członków zespołu CSIRT, jest możliwość reagowania na nie poza własną lokalizacją. Reagowanie poza siedzibą firmy jest dość powszechną praktyką w większych organizacjach, a nawet normą w zespołach CSIRT, które konsultują się z innymi organizacjami. W rezultacie zespoły CSIRT często muszą przeprowadzać cały proces reagowania w innej lokalizacji, bez wsparcia cyfrowego laboratorium kryminalistycznego. Mając na uwadze to wyzwanie, zespoły CSIRT powinny przygotować kilka zestawów przenośnych. Zestawy te są wstępnie skonfigurowane i zawierają sprzęt i oprogramowanie niezbędne do wykonywania działań przez zespół CSIRT podczas reagowania na incydent. Zestawy te powinny być wystarczające do przeprowadzenia całego procesu dochodzenia w zakresie cyberbezpieczeństwa, przy czym zespół CSIRT powinien zidentyfikować bezpieczne lokalizacje w miejscu zdarzenia, w których można przechowywać i analizować dowody.

Zestawy przenośne powinny być mobilne, konfigurowalne tak, by mieściły się w bezpiecznej, twardej walizce i były gotowe do użycia w dowolnym momencie. Zespoły CSIRT powinny dopilnować, by po każdym incydencie zestaw taki był uzupełniany wszelkimi elementami, które zostały użyte podczas ostatniego incydentu. Ponadto sprzęt i oprogramowanie powinny być odpowiednio skonfigurowane, tak by analitycy mieli pewność co do ich dostępności podczas incydentu. Przykład zestawu przenośnego można zobaczyć na rysunku 3.13.

Rysunek 3.13. Zestaw przenośny do zastosowań w kryminalistyce cyfrowej

Przenośny zestaw powinien zawierać co najmniej:

- **Laptop do badań kryminalistycznych**. Laptop powinien zawierać wystarczającą ilość pamięci RAM (32 GB), umożliwiającą wykonanie obrazu dysku twardego w rozsądnym czasie. Laptop powinien również zawierać platformę oprogramowania kryminalistycznego (jak omówiono wcześniej). Jeśli to możliwe, to powinien być również wyposażony w co najmniej jeden kryminalistyczny system operacyjny Linux, taki jak CAINE lub SIFT.
- **Kable sieciowe**. Zestaw kilku kabli CAT5 o różnych długościach może być bardzo przydatny w sytuacji, gdy zespół CSIRT musi uzyskać dostęp do sieci lub połączyć się z jakimkolwiek sprzętem sieciowym, takim jak router lub przełącznik.
- **Fizyczną blokadę zapisu**. Każdy zestaw przenośny powinien mieć fizyczną blokadę zapisu przeznaczoną do tworzenia obrazów dysków twardych, z którymi może się spotkać personel zespołu CSIRT.
- **Zewnętrzne dyski twarde USB**. Zestaw przenośny powinien zawierać kilka dysków twardych USB o pojemności 1 TB lub 2 TB. Mogą one zostać użyte do tworzenia obrazów dysków twardych w potencjalnie zagrożonych systemach.

- **Zewnętrzne urządzenia USB**. Z punktu widzenia kryminalistyki przechowywanie dowodów zebranych z dzienników lub zrzutów pamięci RAM w potencjalnie zagrożonym systemie nie jest uzasadnione. Zestaw przenośny powinien być wyposażony w kilka dysków USB o dużej pojemności (64 GB) do wypakowywania plików dziennika, przechwytywania pamięci RAM lub innych informacji uzyskanych z danych wyjściowych wiersza poleceń.
- **Bootowalny dysk USB lub CD/DVD**. Pomimo że nie są używane w każdym przypadku, posiadanie kilku bootowalnych dystrybucji Linuksa może być przydatne, gdy laptop o przeznaczeniu kryminalistycznym jest wykorzystywany do innych celów.
- **Torby lub pudełka na dowody**. W trakcie trwania incydentu może okazać się, że konieczne będzie przechwycenie dowodu i przetransportowanie go poza miejsce zdarzenia. W rezultacie dobrze jest mieć możliwość zabezpieczenia dowodów na miejscu bez konieczności szukania odpowiedniego pojemnika.
- **Torby antystatyczne**. W przypadku zajęcia dysków twardych jako dowodów należy je przewozić w torbach antystatycznych.
- **Formularze łańcucha dozoru**. Jak omówiono wcześniej, posiadanie formularza łańcucha dozoru dla każdego dowodu ma kluczowe znaczenie. Dysponowanie tuzinem pustych formularzy jest dużo lepszym rozwiązaniem niż szukanie drukarki do wydrukowania nowych kopii.
- **Zestaw narzędzi**. Mały zestaw narzędzi zawierający śrubokręty, szczypce i latarkę jest przydatny w sytuacji, gdy trzeba wymontować dyski twarde, przeciąć połączenia lub uzyskać dostęp analityka do ciemnego zakątka centrum danych.
- **Notatnik i przybory do pisania**. Właściwa dokumentacja ma kluczowe znaczenie. Tworzenie odręcznych notatek długopisem może się wydawać staromodne, jest to jednak najlepszy sposób na zrekonstruowanie wydarzeń w miarę rozwoju incydentu. Posiadanie w zestawie kilku notatników i długopisów gwarantuje, że personel zespołu CSIRT nie będzie musiał szukać tych przedmiotów w sytuacji, gdy właśnie wystąpiło krytyczne zdarzenie. Zestawy przenośne należy inwentaryzować co najmniej raz w miesiącu, tak by były w pełni zaopatrzone i przygotowane do użycia. Powinny być również zabezpieczone i dostępne wyłącznie dla personelu CSIRT. Pozostawione na widoku publicznym zestawy takie są często narażone na zdekompletowanie przez innych pracowników poszukujących śrubokręta, kabla sieciowego lub latarki. W przypadku zespołów CSIRT obsługujących organizacje rozproszone geograficznie dobrym pomysłem jest przygotowanie i umieszczenie takich zestawów w kluczowych lokalizacjach, takich jak główne biura, centra danych lub inne lokalizacje poza siedzibą firmy. Pozwala to uniknąć konieczności przewożenia zestawu samolotem. Przykład niektórych elementów, które należy umieścić w zestawie przenośnym, można zobaczyć na rysunku 3.14.

Gratulujemy pomyślnego ukończenia tego rozdziału!

Rysunek 3.14. Zawartość zestawu przenośnego

Podsumowanie

Reagowanie na incydenty obejmuje szeroki zakres dyscyplin, od prawnych po naukowe. Członkowie zespołu CSIRT odpowiedzialni za przeprowadzanie badań z zakresu kryminalistyki cyfrowej powinni mieć bardzo dobrą wiedzę na temat jej prawnych i technicznych aspektów. Ponadto powinni być zaznajomieni z szeroką gamą narzędzi i urządzeń niezbędnych do pozyskiwania danych, ich badania i raportowania danych uzyskanych podczas badania. Właściwe zastosowanie technik kryminalistycznych ma kluczowe znaczenie do uzyskania wglądu w łańcuch zdarzeń, który doprowadził do wysłania zespołu CSIRT w celu zbadania incydentu. W tym rozdziale na początku omówione zostały różne aspekty prawne kryminalistyki cyfrowej, takie jak reguły dowodowe oraz przepisy dotyczące cyberprzestępczości. W dalszej części przedstawione zostały naukowe podstawy kryminalistyki cyfrowej, dające pojęcie o tym, w jaki sposób techniki te należy stosować w dochodzeniach. Poszerzeniem tej wiedzy były rozważania na temat wpasowania tych technik do ram dochodzeń z zakresu cyberbezpieczeństwa. Na koniec przedstawiony został przegląd różnych narzędzi dostępnych dla badaczy z dziedziny kryminalistyki cyfrowej.

W następnym rozdziale omówione zostało wspólne zastosowanie kryminalistyki cyfrowej wraz z metodą dochodzeniową w celu reagowania na incydenty.

Pytania

1. Co nie jest federalną zasadą dowodową?
   A. Test na obecność odpowiednich dowodów.
   B. Reguła Locarda.
   C. Zeznanie biegłych.
   D. Reguła najlepszego dowodu.
2. Należy zachować odpowiedni łańcuch dozoru, by zapewnić integralność dowodów cyfrowych.
   A. Prawda
   B. Fałsz
3. Jakie elementy powinny znaleźć się w zestawie do kryminalistyki cyfrowej?
   A. Fizyczna blokada zapisu.
   B. Notatnik i długopis.
   C. Kable sieciowe.
   D. Wszystkie powyższe.
4. Co NIE jest częścią procesu kryminalistycznego?
   A. Identyfikowanie.
   B. Zeznanie na sali sądowej.
   C. Zabezpieczanie.
   D. Analizowanie.

Lektura uzupełniająca

- Materiał ISACA na temat kryminalistyki cyfrowej: *https://www.isaca.org/isaca-digital-videos/archive/overview-of-digital-forensics*.
- Zarys historyczny FBI CART: *https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=137561*.

Skorowidz

A

B

C

D

E

M

N

O

P

R

S

T

U

V

W

X

Y

Z

Przygotuj się, znajdź i zlikwiduj zagrożenie!

Informatyka śledcza zapewnia narzędzia nie tylko prowadzącym dochodzenia kryminalne, ale również specjalistom do spraw cyberbezpieczeństwa. Na tym polu trwa ciągły wyścig zbrojeń między nimi a przestępcami, gdyż konsekwencje udanego ataku mogą się okazać niezwykle poważne. Umiejętność poprawnego reagowania na incydenty bezpieczeństwa jest tu kluczową sprawą.

Ta książka jest przewodnikiem dla profesjonalistów w dziedzinie cyberbezpieczeństwa. Przedstawia podstawowe zasady reagowania na incydenty bezpieczeństwa i szczegółowo, na przykładach, omawia proces tworzenia zdolności szybkiej i skutecznej reakcji na takie zdarzenia. Zaprezentowano tu techniki informatyki śledczej, od pozyskiwania dowodów i badania pamięci ulotnej po badanie dysku twardego i dowodów pochodzących z sieci. Szczególną uwagę poświęcono zagrożeniom atakami ransomware. Nie zabrakło omówienia roli analizy zagrożeń w procesie reagowania na incydenty, a także zasad sporządzania raportów dokumentujących reakcję na incydent i wyniki analizy. Pokazano również, w jaki sposób prowadzi się polowania na zagrożenia.

Z tą książką:

- zbudujesz zdolność reagowania na incydenty w swojej organizacji
- nauczysz się poprawnego zbierania i analizowania dowodów
- zintegrujesz techniki i procedury śledcze z ogólnym procesem reagowania na incydenty
- przyswoisz różne metody polowania na zagrożenia
- opanujesz sposoby tworzenia raportów z incydentów
- wdrożysz odpowiednie praktyki reagowania na ataki ransomware

Gerard Johansen od ponad piętnastu lat zajmuje się informatyką śledczą. Jako analityk bezpieczeństwa współpracował z organizacjami z różnych branż, od opieki zdrowotnej po finanse. Posiada kilka certyfikatów branżowych z zakresu kryminalistyki cyfrowej, analizy zagrożeń i cyberbezpieczeństwa. Obecnie zarządza zespołem specjalistów do spraw obsługi incydentów.

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 978-83-289-0432-3
9 788328 904323
Cena: 99,00 zł