UJAWNIANIE I ZABEZPIECZANIE ŚLADÓW CYFROWYCH V

1. Ogólna charakterystyka ujawniania i zabezpieczania śladów cyfrowych

Sposób zabezpieczania śladów cyfrowych przypomina metody stosowane przy innych rodzajach śladów, występujących na miejscu oględzin i miejscach innych czynności procesowych (np. przeszukania). Ogólne zasady stosowane w przypadku znalezienia materiału do badań komputerowych skupiają się na wezwaniu eksperta (biegłego) z zakresu kryminalistyki informatycznej. Osoby uczestniczące w procesie zabezpieczania śladów cyfrowych powinny posiadać wiedzę w dziedzinie informatyki i posiadać wiedzę o specyfikacji urządzenia, na którym będą dokonywane czynności. Większość przypadków utraty lub zatarcia istotnych śladów powstaje na poziomie zabezpieczania urządzeń cyfrowych i danych komputerowych przez zastosowanie błędnej procedury. Zalecane jest przed przystąpienie do zabezpieczania precyzyjne ustalenie określonych informacji: jakie dane należy zabezpieczyć, gdzie się one znajdują i dokonać odpowiednich przygotowań. Niektóre rodzaje urządzeń można zabezpieczyć w tradycyjny sposób, jak np. telefony komórkowe i przeprowadzić analizę w laboratorium kryminalistycznym, inne urządzenia natomiast wymagają zastosowania specjalistycznych urządzeń na miejscu ich znalezienia.

Ekspert z zakresu informatyki kryminalistycznej powinien:

1. Zebrać informacje na temat sprzętu i środowiska komputerowego, które ma zostać poddane badaniu, tj.: rodzajów komputerów, systemów operacyjnych, programów użytkowych, rodzajów pamięci, konfiguracji sieci, haseł dostępu itp.

2. Ustalić okoliczności, w jakich sprzęt będzie zabezpieczany, np. podczas przeszukania, w obecności użytkowników sprzętu komputerowego lub pod ich nieobecność, czy będą dostępni administratorzy systemu itp.
3. Sprawdzić stan aktywności systemów komputerowych, w szczególności, czy system jest włączony, wyłączony, w trakcie backupu itp.
4. Przewidzieć i zapobiec możliwości zdalnego usunięcia danych[226].
5. Nie przechowywać w bezpośredniej bliskości urządzeń takich jak telefony, radio itp., mogących wpłynąć negatywnie lub zakłócić pracę zabezpieczanego urządzenia.
6. Jeżeli urządzenie jest wyłączone, pod żadnym pozorem nie należy włączać zasilania – może to spowodować utratę danych przechowywanych w pamięci krótkotrwałej przez zainicjowanie startu systemu. Włączenie sprzętu powinno odbywać się w ściśle kontrolowanym środowisku kryminalistycznego laboratorium informatycznego po wcześniejszym zabezpieczeniu pamięci wirtualnej.
7. Jeżeli w systemie rozpoczęta jest procedura np. drukowania, należy pozwolić maszynie ją dokończyć. Nie można zamykać również uruchomionych programów.

W przypadku urządzeń wyposażonych w system operacyjny, np. Windows/Linux, pomocne może okazać się umożliwienie działań osobie posiadającej wiedzę na temat topografii i zasad funkcjonowania obecnego na urządzeniu systemu. Współczesne komputery osobiste są najczęściej wyposażone w systemy nowszych generacji, zdarzają się jednak sytuacje, gdy komputer posiada system starszej generacji, który nie jest w obecnych czasach powszechnie wykorzystywany. W takich sytuacjach przydatne może okazać się zapoznanie z dokumentacją na temat struktury wewnętrznej systemu ze źródeł, jakimi są instrukcja i literatura specjalistyczna, przed próbą dokonania zabezpieczenia śladów cyfrowych. Przystępując do zabezpieczania komputera i każdego innego urządzenia cyfrowego, w pierwszej kolejności należy całkowicie odciąć możliwość korzystania z danego sprzętu przez osobę postronną. Ma to znaczenie priorytetowe dla bezpieczeństwa danych zawartych w pamięci cyfrowej i odnosi się zarówno do ingerencji na miejscu oględzin, jak i zdalnej próbie nieautoryzowanego wejścia do sytemu na odległość. Działania takie mogą zapobiec ewentualnym konsekwencjom destrukcyjnym w stosunku do zabezpieczanych danych i przejęciu zdalnej kontroli nad urządzeniem. Najprostszą metodą przeciwdziałania jest odłączenie sprzętu od dostępu do sieci. W dalszej kolejności należy ustalić ilość jednostek centralnych i lokalizację wszystkich urządzeń peryferyjnych współpracujących z zabezpieczanym urządzeniem. Istotne jest również ustalenie rodzaju i topologii sieci, do której sprzęt był podłączony, rodzaju nośników

[226] J. Moszczyński: *Informatyka kryminalistyczna*, [w:] *Kryminalistyka – czyli rzecz o metodach śledczych*, red. E. Gruza, M. Goc, J. Moszczyński, Warszawa 2008, s. 569.

pamięci, jakie wykorzystuje i jest w stanie obsługiwać, sposobu archiwizacji danych. W tym momencie warto nadmienić o dwóch aspektach łatwych do przeoczenia. Po pierwsze, miejsce oględzin i zabezpieczania sprzętu komputerowego wcale nie musi odnosić się w całości do komputera i urządzeń z nim połączonych. Funkcjonariusze powinni dokładnie sprawdzić otoczenie w poszukiwaniu wszelkich innych nośników danych, jak np. płyty CD/DVD, pamięć przenośna itp. zlokalizowane w otoczeniu urządzenia docelowego. Warto przeszukać całe pomieszczenie, biurka, szuflady itp. Paradoksalnie najistotniejsze ślady cyfrowe mogą znajdować się np. na płycie CD leżącej obok komputera. Drugą sprawą, obok której nie można przejść obojętnie, jest wykorzystanie innych dziedzin techniki kryminalistycznej w stosunku do urządzeń cyfrowych. Przed dokonaniem zabezpieczenia np. komputera należy sprawdzić, czy nie znajdują się na nim ślady linii papilarnych, jeżeli w danym konkretnym przypadku będzie to miało znaczenie dla danej sprawy. Ślady daktyloskopijne mogą ulec zatarciu, jeżeli ekspert od spraw informatyki rozpocznie swoje działania. Najczęstszym potencjalnym miejscem występowania śladów linii papilarnych będą klawiatura, myszka, okolice włączników monitora i komputera, te miejsca na obudowie urządzenia, które zawierają przyciski i tylna strona sprzętu odpowiedzialna za okablowanie (szczególnie w przypadku wykrycia podłączonego urządzenia szpiegowskiego i wykradającego dane). Ekspert z zakresu daktyloskopii, działając razem z ekspertem z zakresu informatyki, powinien stosować takie metody i środki ujawniania śladów linii papilarnych, które nie uszkodzą danego sprzętu[227]. W konkretnych przypadkach, na urządzeniach komputerowych mogą występować i inne ślady kryminalistyczne, np. ślady mechanoskopijne (gdy sprawca usiłował dostać się do wnętrza urządzenia, stosując różnego rodzaju narzędzia), ślady biologiczne (np. ślady krwi itp.). Dopiero po zweryfikowaniu wszystkich tych danych i zebraniu informacji można przystąpić do stopniowego zamykania systemu i późniejszego odłączenia od prądu urządzenia.

W pierwszej kolejności należy:

1. Zapisać otwarte pliki pod nową nazwą (lub wykorzystać archiwizację danych) na zewnętrznym nośniku (wykluczone jest zapisywanie jakichkolwiek plików na dysku sprawdzanego komputera ze względu na możliwość nadpisania danych skasowanych wcześniej przez użytkownika) – w ten sposób zachowujemy zmiany wprowadzone do pliku.

---

[227] Praca nie zawiera omówienia metod i środków ujawniania śladów linii papilarnych na urządzeniach komputerowych, gdyż stosuje się metody ogólne opisywane już w specjalistycznej literaturze przedmiotu, por. np. J. Moszczyński: *Daktyloskopia,* Warszawa 1997, s. 52 i nast., J. Kasprzak: *Kryminalistyka. Podręcznik dla Żandarmerii Wojskowej, cz. I, Technika kryminalistyczna,* Warszawa 1995, s. 28 i nast., E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka – czyli rzecz o metodach śledczych,* Warszawa 2008, s. 310 i nast., M. Kobylas: *Dermatoskopia,* Szczytno 2005, s. 32 i nast.

2. Zamknąć pliki (zapisując przedtem ich nazwę na kartce, pomoże to w późniejszym odtworzeniu, co i w jakim czasie było uruchomione na komputerze), nie zachowując zmian – w ten sposób zachowujemy oryginał pliku.
3. Wszystkie te czynności szczegółowo opisać w protokole, podając nazwy plików oraz oznaczenia nośników, na jakich zostały zapisane (opisywać również krok po kroku, jakie działania zostały powzięte)[228].
4. Dokonać fotografii stanu monitora w taki sposób, by na zdjęciu widoczne były wszelkie informacje wyświetlone na urządzeniu (operację taką należy powtarzać przy każdej zmianie dokonywanej w systemie, mającej swoje odzwierciedlenie w zapisie na wyświetlaczu – zabieg taki ma na celu wprowadzić dodatkowe zabezpieczenie przed późniejszymi ewentualnymi błędami, mogącymi spowodować bezpowrotną utratę danych zawartych w pamięci urządzenia). Fotografii należy dokonywać urządzeniem zewnętrznym, np. aparatem fotograficznym, nie można robić zrzutów ekranu w systemie operowanego urządzenia, by nie wprowadzać zmian w historii pamięci.

Po ukończeniu szczegółowego dokumentowania można przystąpić do wstępnego rozmontowywania sprzętu komputerowego w celu przetransportowania do specjalistycznego laboratorium kryminalistycznego i pracowni informatycznej. W trakcie przeprowadzania tej części operacji należy zwrócić uwagę na wszelkie zapiski znajdujące się w bliskiej odległości od sprzętu cyfrowego, materiały takie mogą zawierać hasła i dane potrzebne do uwierzytelnienia użytkownika systemu. W trakcie rozłączania kabli należy oznakować je w taki sposób, by można było odwzorować pierwotne ich ułożenie – wiele współczesnych komputerów dysponuje licznymi gniazdami USB. Sprzęt i materiały zabezpieczone do badań komputerowych należy zarejestrować metodą fotograficzną lub wideo w ich pierwotnym stanie, uwzględniając:

1. Ogólny wygląd miejsca przeprowadzania czynności.
2. Sprzęt komputerowy i sposób połączenia jego elementów.
3. Nośniki danych.
4. Stan ekranu monitora.
5. Stan przełączników, diod i innych wskaźników.

Wszystkie rozmontowane komponenty urządzenia cyfrowego powinny zostać odpowiednio zapakowane, by wykluczyć ryzyko uszkodzenia lub całkowitego ich zniszczenia w trakcie transportu. Elementy takie, jak klawiatura, myszka, monitor, stacja centralna, kable muszą zostać odpowiednio opakowane i zabezpieczone przed uszkodzeniami mechanicznymi. Dyski i pamięci należy odizolować za pomocą folii ochronnej i unikać kontaktów z przedmiotami mogącymi wywoływać pole magnetyczne. Wszystkie elementy powinny być także szczelnie zamknięte i zaplombowane na miejscu w celu zminimalizowania ryzyka dostępu do zabez-

[228] J. Moszczyński: op. cit., s. 570.

pieczonych danych przez osoby nieupoważnione. Tak zabezpieczone materiały powinny zostać niezwłocznie przetransportowane do odpowiedniej placówki zajmującej się analizą danych cyfrowych.

2. Zabezpieczanie urządzeń teleinformatycznych

Zabezpieczanie śladów cyfrowych wiąże się z wymogiem posiadania specjalistycznej wiedzy na temat szerokiej gamy urządzeń cyfrowych. Procedury wymagane przy pracy ze sprzętem elektronicznym będą się od siebie różnić w zależności od tego, jakie urządzenie trzeba w danej chwili zabezpieczyć. Zastosowanie tej samej metody w różnych przypadkach może być katastrofalne w skutkach dla śladów cyfrowych. Dodatkowo ekspert z zakresu informatyki kryminalistycznej musi wiedzieć, jakie potencjalne dowody można uzyskać z określonych urządzeń. Wiedza taka wydaje się także konieczna dla przedstawicieli organów ścigania, przede wszystkim techników kryminalistyki. Dlatego też ta część rozdziału będzie poświęcona opisaniu odpowiednich metod zabezpieczania i obchodzenia się ze sprzętem elektronicznym różnego typu: komputerem stacjonarnym (dotyczy to także laptopa), telefonem komórkowym, innym sprzętem łączności, elektronicznym sprzętem biurowym oraz akcesoriami komputerowymi (kartami, płytami CD/DVD, przenośnymi nośnikami pamięci).

Współcześnie nie jesteśmy w stanie wskazać w sposób wyczerpujący wszystkich przypadków zabezpieczanego sprzętu informatycznego i wszystkich szczegółowych zasad postępowania. Ujęte zostały jedynie problemy najważniejsze. Ścisłe procedury zabezpieczania nie zostały do chwili obecnej szczegółowo skatalogowane i opisane w literaturze przedmiotu. Z jednej strony eksperci z zakresu informatyki kryminalistycznej nie są zbyt wylewni i dość niechętnie dzielą się wiedzą i swoimi metodami pracy, z drugiej zaś strony (chyba to ważniejszy powód), stosowane metody bardzo szybko ulegają zmianie czy modyfikacji, w zależności od poziomu rozwoju techniki i informatyki. Przedstawione poniżej procedury zostały opisane na podstawie materiałów uzyskanych z rozmów i wywiadów przeprowadzonych z ekspertami informatyki kryminalistycznej.

Procedura zabezpieczania różnego rodzaju komputerów:

1. Zabezpieczyć miejsce znalezienia komputera przed osobami postronnymi.
2. Uniemożliwić łączenie się z komputerem w sposób tradycyjny i zdalny przez odłączenie łącza telefonicznego/internetowego.

3. Jeżeli znaleziony komputer jest wyłączony, pod żadnym pozorem nie można go włączać do czasu przybycia eksperta.
4. Jeżeli komputer jest włączony (komputer stacjonarny i przenośny), należy powstrzymać się od wszelkich ingerencji w systemie i skonsultować się z ekspertem.

W przypadku, gdy na miejscu oględzin nie przebywa ekspert z zakresu zabezpieczania urządzeń cyfrowych, należy:

1. Sfotografować zastany stan monitora, całość sprzętu komputerowego i sposób podłączenia kabli.
2. W następnej kolejności należy odłączyć kabel zasilający – spowoduje to natychmiastowe wyłączenie się maszyny, ale nie wpłynie negatywnie na zawarte dane newralgiczne, które mogłyby zostać usunięte przy tradycyjnym wyłączeniu komputera.
3. Komputery przenośne są najczęściej wyposażone w system zasilania z baterii. Jeżeli laptop nie wyłączył się pod odłączeniu kabla zasilającego, należy odłączyć baterię od bazy. Bateria najczęściej znajduje się na spodzie komputera lub w tylnej jego części. Część ta jest demontowana za pomocą przełącznika mechanicznego lub schowana pod przykręconą płytką. Po usunięciu baterii nie można podłączać jej do czasu przybycia eksperta.
4. Należy zabezpieczyć wszystkie możliwe otwory cyfrowe i analogowe przy użyciu plomb.
5. W celu jak najlepszego odwzorowania pierwotnego podłączenia kabli i urządzeń cyfrowych do komputera wymagane jest sporządzenie szkicu przedstawiającego schemat połączeń.
6. Wszystkie końcówki kabli powinny zostać dokładnie opisane, wyszczególniając typ pochodzenia, np. USB 2.0, Micro USB itp.
7. Jeżeli zachodzi potrzeba przetransportowania komputera, należy spakować każdy z elementów oddzielnie i zabezpieczyć przed potencjalnymi uszkodzeniami mechanicznymi. Pudełka zawierające elementy komputerowe muszą zostać odpowiednio opisane i opieczętowane.
8. Urządzenia komputerowe trzeba trzymać w bezpiecznym miejscu, z dala od źródeł pola magnetycznego, przekaźników radiowych i innych potencjalnie niebezpiecznych źródeł.
9. Poza kablami i stacją główną należy zabezpieczyć wszystkie komponenty dodatkowe, np. klawiaturę, myszkę, drukarkę, skaner, monitor itp.
10. Dodatkowo, jeżeli jest to możliwe, należy zabezpieczyć wszelkie odnalezione dokumenty związane ze sprzętem elektronicznym, instrukcje obsługi, karty programowe, opisy komponentów wewnętrznych itp.
11. W celu ułatwienia pracy ekspertom z zakresu informatyki, należy w miarę możliwości uzyskać i zanotować wszelkie hasła i loginy. Dane takie mogą być w posiadaniu osób korzystających z komputera lub znajdować się w bezpośrednim jego sąsiedztwie.

Jednym z wyjątków są komputery znajdujące się w biurach i serwerowniach – w takich wypadkach bezwzględnie należy skontaktować się z ekspertem i poczekać na jego przybycie.

1. Działania należy ograniczyć od zabezpieczenia komputera od osób postronnych.
2. Nie wolno wyłączać zasilania komputera, nawet przez wyciągnięcie wtyczki zasilającej. Podjęcie podobnych działań może skutkować ciężkim uszkodzeniem systemu, zakłóceniem legalnie działającego systemu biurowego i spowodować konsekwencje prawne wobec osoby (funkcjonariusza), który dopuści się takiej czynności.

Procedura zabezpieczania telefonów komórkowych:

1. W przypadku odnalezienia telefonu komórkowego, należy zabezpieczyć dostęp do urządzenia przez osoby postronne.
2. Jeżeli telefon jest wyłączony, pod żadnym pozorem nie należy go włączać. Uruchomienie urządzenia może uruchomić wewnętrzne systemy bezpieczeństwa i w efekcie w dużym stopniu utrudnić późniejszą pracę ekspertów.
3. Należy opisać i sfotografować całą zawartość wyświetlacza, zwracając uwagę na wszystkie informacje zawarte na nim w danej chwili.
4. Jeżeli jest to możliwe, trzeba ustawić priorytet niskiego poboru energii w systemie telefonu na potrzeby transportu.
5. Po zatrzymaniu urządzenia natychmiast skontaktować się z dostawcą usługi w celu blokady numeru i uzyskania dalszych potrzebnych informacji dla prawidłowego toku śledztwa.
6. W przypadku nieumyślnego zablokowania telefonu wymagana jest ingerencja pracownika firmy dostarczającej usługi telefoniczne w celu odblokowania telefonu.
7. Poza telefonem, należy zabezpieczyć w miarę możliwości wszystkie komponenty związane z urządzeniem, np. instrukcję obsługi, okablowanie, ładowarkę itp.
8. W celu zachowania spójności danych należy poczynić wszelkie starania, by telefon nie został w całości rozładowany – może to spowodować utratę pewnych newralgicznych danych zawartych w systemie.
9. Należy zabezpieczyć urządzenie przed nadmiernym zimnem, ciepłem, polem magnetycznym, źródłami emitującymi silne fale radiowe i przed wszystkimi innymi czynnikami mogącymi wywołać negatywne efekty.
10. Telefon należy starannie opisać i umieścić w bezpiecznym opakowaniu tymczasowym, mając na uwadze poziom baterii.
11. Odłączyć telefon od sieci, uniemożliwiając zdalne nim sterowanie.
12. Prowajder usługi ma obowiązek dostarczyć wszelkie potrzebne funkcjonariuszom informacje.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione w telefonie komórkowym:

1. Numery telefonów.
2. Dane kontaktowe i adresy.
3. Informacje o połączeniach przychodzących i wychodzących.
4. Daty i godziny wykonywanych połączeń.
5. Kody PIN.
6. Wiadomości tekstowe i audio.
7. Numery kart debetowych i powiązanymi metodami płatności online.
8. Dane dostępu do poczty mailowej i Internetu.
9. Historia przeglądarki internetowej.
10. Informacje serwisowe od prowajdera usługi.
11. Dane i numery karty telefonicznej.
12. Materiały audio, video, foto zawarte w pamięci urządzenia.
13. Inne cenne informacje zawarte na ekranie urządzenia w chwili jego zabezpieczenia.
14. Dane zainstalowanych aplikacji
15. Logi systemowe oraz zainstalowanych aplikacji.

Telefony bezprzewodowe nadal pozostają jednymi z bardziej rozpowszechnionych modeli aparatów telefonicznych. Charakteryzują się budową umożliwiającą korzystanie z przenośnej słuchawki w obszarze działania nadajnika z podłączeniem do sieci teleinformacyjnej. W przypadku zabezpieczania śladów cyfrowych z przedstawionego urządzenia należy mieć na uwadze, że składa się on z minimum dwóch komponentów, które mogą zawierać odmienne dane cyfrowe. Telefony tego rodzaju są rozpowszechnione w gospodarstwach domowych i biurach, umożliwiają precyzyjnie łączenie w wewnętrznej sieci biurowej pomiędzy określonymi pracownikami. Obecne są również przypadki, gdzie telefony bezprzewodowe stanowią zupełnie odrębną siec teleinformacyjną odciętą od głównej magistrali połączeń. Najczęściej takie rozwiązanie dotyczy dużych biurowców i firm posiadających własne systemy komunikacyjne. Jedna baza urządzenia wyposażona w nadajnik jest w stanie obsługiwać kilka telefonów równocześnie.

Procedura zabezpieczania telefonów bezprzewodowych:

1. W pierwszej kolejności należy odciąć dostęp do urządzenia wszystkim osobom postronnym.
2. Jeżeli urządzenie jest włączone, nie należy go wyłączać pod groźbą utraty danych cyfrowych.
3. Wyłączenie lub dopuszczenie do całkowitego rozładowania się urządzenia może spowodować blokadę wewnętrzną systemu.
4. Należy skatalogować, sfotografować i opisać wszystkie elementy składowe zabezpieczanego urządzenia.

5. Jeżeli telefon jest wyposażony w wyświetlacz, wymagane jest dokładnie sfotografowanie jego aktualnego stanu tak, by były widoczne wszystkie informacje wyświetlane na ekranie.
6. Jeżeli jest to możliwe, należy zmienić priorytet pracy urządzenia na pobierający jak najmniejszą ilość energii.
7. W przypadku, gdy urządzenie jest wyłączone, należy pozostawić je w takim stanie – inicjowanie zasilania może spowodować nadpisanie pewnych danych zawartych w pamięci telefonu, podobnie jak w przypadku komputerów osobistych.
8. Zabezpieczone urządzenia należy przechowywać w taki sposób, by nie narazić ich na uszkodzenia mechaniczne i cyfrowe. Wymagane jest unikanie miejsc posiadających znaczne oddziaływanie magnetycznie i innych mogących zagrozić danym cyfrowym.
9. Wszystkie komponenty telefonu powinny być oddzielnie spakowane i zaplombowane w celu transportu do laboratorium kryminalistyki informatycznej.
10. Telefon powinien być jak najszybciej dostarczony do specjalistycznej analizy, by uniknąć rozładowania akumulatora energii.
11. Zabezpieczanie bazy z nadajnikiem może się odbywać na zasadach i procedurach używanych przy komputerach stacjonarnych.
12. W celu zmaksymalizowania zebranych informacji należy uzyskać od pracowników i osób korzystających z telefonu bezprzewodowego wszystkie możliwe dane wymagane do uwierzytelniania.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione w telefonie bezprzewodowym:

1. Numery połączeń przychodzących i wychodzących.
2. Skrzynka adresatów.
3. Historia połączeń.
4. Daty i godziny połączeń.
5. Numery serwisowe.
6. Dane personalne i adresy.
7. Numery PIN.
8. Wiadomości tekstowe.
9. Skrzynka poczty mailowej.
10. Numery kart powiązanych z urządzeniem.
11. Inne odnalezione informacje.

Urządzenie nazywane automatyczną sekretarką ma za zadanie rejestrować połączenia przychodzące i pozwala na zostawienie wiadomości głosowej. W dzisiejszych czasach znakomita większość nowoczesnych aparatów telefonicznych posiada wbudowane funkcje automatycznej sekretarki. Zdarzają się jednak modele telefonów stacjonarnych lub biurowych z podłączonymi oddzielnymi sekre-

tarkami. Różnica pomiędzy wbudowaną opcją sekretarki a urządzeniem o ściśle sprecyzowanej funkcji polega na ilości przechowywanych danych i większej liczbie opcji użytkownika. Duża liczba stacjonarnych sekretarek posiada funkcję nagrywania rozmów na pamięć przenośną lub inne nośniki danych.

Procedury zabezpieczania automatycznych sekretarek:

1. Jeżeli urządzenie jest włączone, nie można go wyłączać – może to spowodować negatywne skutki dla danych zawartych w pamięci tak samo, jak w poprzednio opisywanych urządzeniach.
2. Należy niezwłocznie odłączyć automatyczną sekretarkę od linii telefonicznej. Wszelkie dodatkowe potencjalne wiadomości, jakie mogą nadejść, są w stanie nadpisać już istniejące i zapisane w pamięci urządzenia.
3. Sfotografować i szczegółowo opisać zabezpieczany sprzęt, zwracając szczególną uwagę na model urządzenia.
4. Jeżeli automatyczna sekretarka posiada funkcję zgrywania danych na pamięć podręczną (pendrive, płyty CD), bezwzględnie trzeba przeprowadzić taką operację. Pozwoli to na zabezpieczenie pod postacią dodatkowej kopii wszystkich zawartych na urządzeniu materiałów audio.
5. Należy poczynić wszelkie starania, by automatyczna sekretarka nie rozładowała się do momentu analizy specjalistycznej.
6. Włączenie urządzenie w przypadku, gdy jest ono wyłączone, może spowodować podobne konsekwencje, jak w przypadku komputerów.
7. Urządzenie należy zabezpieczyć i zaplombować, by zminimalizować szansę na ingerencję osoby nieupoważnionej. Następnie trzeba przewieźć tak szybko, jak to tylko możliwe, sprzęt do analizy.
8. W przypadku odnalezienia dokumentów dotyczących urządzenia, je również należy zabezpieczyć.
9. Tak jak w przypadku większości urządzeń teleinformatycznych, wszelkie oddziaływania, takie jak silne pole magnetyczne, niska i wysoka temperatura, mogą uszkodzić dane cyfrowe – należy dokonać wszelkich starań, by unikać takich sytuacji.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione w automatycznej sekretarce:

1. Zapisy audio.
2. Przychodzące i wychodzące połączenia.
3. Numery telefonów i adresy.
4. Dane personalne.
5. Połączenia z domową lub biurową siecią teleinformatyczną.
6. Inne elementy, podobne jak w przypadku telefonów komórkowych i stacjonarnych.

Caller ID Device jest urządzeniem rzadko występującym w naszym kraju. Jego działanie polega na sprawdzaniu przychodzących połączeń i umożliwia au-

tomatyczne ich rejestrowanie za pośrednictwem komputera. Najczęstszym zastosowaniem Caller ID Device jest blokowanie niechcianych połączeń. Urządzenie wyświetla źródło i numer przychodzący, dane nadawcy i godzinę. Możliwe jest ustawienie stopnia prywatności, by zautomatyzować odrzucanie połączeń niechcianych, np. ofert reklamowych. Drugą funkcją jest rejestrowanie połączenia i przesyłanie go do pamięci komputera.

Procedura zabezpieczania Caller ID Device:

1. Podobnie jak w przypadku innych urządzeń cyfrowych, jeżeli zabezpieczany sprzęt jest wyłączony, pod żadnym pozorem nie powinno się go włączać. Może to spowodować modyfikację danych zawartych w pamięci urządzenia.
2. Należy opisać i skatalogować wszystkie informacje zawarte w pamięci urządzenia, dotyczące odebranych połączeń i nadawców.
3. Jeżeli to możliwe, powinno się przeszukać otoczenie w celu uzyskania dokumentów odnoszących się do zabezpieczanego sprzętu, w szczególności instrukcje obsługi i materiały zawierające hasła i PINy.
4. Urządzenie powinno zostać zapakowane i przewiezione do celów analizy danych, wytyczne na temat ochrony nie odbiegają od już przedstawionych we wcześniejszych opisach sprzętu.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:

1. Liczne dane przychodzące, zawierające numery kontaktowe, adresy i dane personalne.
2. Data i godzina odebranych połączeń.

Podstawową cechą i funkcją Eletronic Paging Device (pager) jest odbieranie krótkich impulsów teleinformatycznych, mających przekazać właścicielowi urządzenia określoną wiadomość. Niektóre z występujących modeli potrafią nadać komunikat zwrotny do adresata. Z punktu widzenia informatyki śledczej i kryminalistyki pozwala to na stworzenie sieci użytkowników powiązanych z badanym urządzeniem.

Procedury zabezpieczania Eletronic Paging Device:

1. W przypadku, gdy zabezpieczane urządzenie pozostaje wyłączone, nie należy go uruchamiać do czasu dostarczenia sprzętu do analizy.
2. Jeżeli urządzenie jest włączone, należy je wyłączyć, zapobiegnie to odbieraniu nowych sygnałów mogących wprowadzić zmiany w pamięci urządzenia.
3. Należy sfotografować i dokładnie opisać stan urządzenia w chwili jego zabezpieczania, uwzględniając także treści wyświetlane na wyświetlaczu.
4. Sprzęt należy umieścić w bezpiecznym pojemniku, chroniącym urządzenie od skutków ubocznych i potencjalnych ingerenci osób nieupoważnionych.
5. Pager powinien zostać jak najszybciej przetransportowany do analizy.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:

1. Numery pagerów. Urządzenie do celów komunikacji posługuje się cyfrowymi numerami. Każdy adresat posiada swój indywidualny numer.

2. Numery Alpha – w odróżnieniu od tradycyjnych – mogą zawierać nie tylko sam numer adresata,ale także krótkie widomości tekstowe lub listy elektroniczne.
3. Niektóre rodzaje pagerów są wyposażone w funkcję przekazywania krótkich wiadomości głosowych, czyli materiałów audio.
4. W przypadku, gdy pager posiada funkcję komunikacji zwrotnej, możliwe jest łatwe ustalenie powiązań połączeń.
5. Inne dane mogące znajdować się w pamięci urządzenia.

Telefaksy są obecnie bardzo popularnymi sprzętami biurowymi, znajdującymi się na wyposażeniu większości istniejących biur. Główną funkcją tych urządzeń jest przesyłanie dokumentów tekstowych, znajdujących się na papierze poprzez zeskanowanie ich treści i wydrukowanie duplikatu u adresata pliku cyfrowego. Dodatkowo telefaksy są urządzeniami wyposażonymi w znaczną ilość pamięci cyfrowej, pozwalającej na przechowywanie zeskanowanych dokumentów.

Procedury zabezpieczania telefaksów:

1. Jeżeli telefaks jest wyłączony, należy pozostawić go w takim stanie.
2. W przypadku zabezpieczania włączonego urządzenia w pierwszej kolejności należy odizolować telefaks od wszystkich osób postronnych, mogących użyć sprzętu. Nie wolno wyłączyć działającego urządzenia, by nie zostały stracone dane przechowywane w pamięci krótkotrwałej. Kolejnym etapem postępowania z włączonym telefaksem musi być podpięcie dysku przenośnego i zgranie na niego całej zawartość przechowywanej pamięci urządzenia – dotyczy to głównie ostatnio faksowanych dokumentów, których dane nie zostały jeszcze skasowane (wszystkie dokumenty wprowadzenie do telefaksu posiadają kopię cyfrową przechowywaną w pamięci krótkotrwałej; jeżeli nie zostaną zapisane w pamięci trwałej, to po wyłączeniu urządzenia dane takie zostaną bezpowrotnie utracone).
3. Sfotografować stan wyświetlacza i całe urządzenie, dodatkowo dokładnie opisując jego stan, typ, informacje wyświetlane na ekranie wyświetlacza.
4. Należy sprawdzić, czy kabel telefoniczny jest podłączony do telefaksu i w przypadku potwierdzenia, należy go odłączyć.
5. Podobną operację trzeba przeprowadzić z kablem umożliwiającym podłączenie do komputera.
6. Wszystkie instrukcje obsługi i inne dokumenty powiązane z telefaksem powinny zostać dodatkowo zabezpieczone.
7. Jeżeli nie ma możliwości zabezpieczenia pamięci włączonego telefaksu, należy zabezpieczyć urządzenie od osób postronnych, odłączyć sieć komputerową i telefoniczną do czasu przybycia eksperta z zakresu informatyki.
8. Wiele telefaksów wymaga podłączenia do komputera w celu optymalnej pracy. Komputer wykorzystywany jako baza może być źródłem cennych informacji – również powinien zostać zabezpieczony w oparciu o procedury dotyczące zabezpieczania komputerów stacjonarnych lub przenośnych.

9. Wszystkie elementy urządzenia w przypadku, gdy jest ono wyłączone, powinny zostać spakowane, wliczając w to kable i komponenty dodatkowe.
10. Całość zabezpieczonych elementów musi zostać przetransportowana w celu szczegółowej analizy informatycznej.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:

1. Lista adresów.
2. Historia przesłanych plików i nawiązanych połączeń.
3. Zasoby pamięci zawierające przychodzące i wychodzące pliki w postaci cyfrowej.
4. Logi zawierające historię transmisji wychodzących i przychodzących.
5. Nagłówki i tytuły przesyłanych informacji.
6. Daty i godziny wykonanych poleceń.

Karty magnetyczne stały się niezwykle popularną metodą identyfikacji człowieka. Pozwalają na autoryzowanie transakcji lub uzyskanie dostępu do określonych miejsc. Karty zawierają czytniki magnetyczne lub w bardziej zaawansowanej formie – małe chipy (mikroprocesory). Większość istniejących kart magnetycznych jest przypisana do określonej osoby. W przypadku kradzieży lub posługiwania się kartą przez osobę trzecią, niebędącą właścicielem karty, można to w bardzo łatwy sposób wykryć. Szczególnie przydatne jest blokowanie możliwości karty bankowych w przypadku ich kradzieży.

Procedury zabezpieczania karty magnetycznej i chipowej:

1. Sfotografować kartę po obydwu stronach, dodatkowo opisać firmę, właściciela i utrwalić wszystkie inne widniejące na karcie dane.
2. Sprawdzić, kto jest właścicielem karty. Można tego dokonać przez odczytanie podpisu właściciela wygrawerowanego na karcie lub kontaktując się z odpowiednią placówką, zajmującą się daną kartą.
3. Sprawdzić, czy zabezpieczana karta jest aktywna i kiedy wygaśnie jej termin przydatności.
4. Ustalić, kto był w posiadaniu karty w chwili jej odnalezienia.
5. Kartę magnetyczną należy zapakować w szczelny pojemnik i przetransportować do analizy.
6. W przypadku karty magnetycznej o przeznaczeniu innym niż środek płatniczy, np. karta dostępu, w pierwszej kolejności należy ustalić odpowiedzi na pięć podstawowych pytań:
   a) Kto wydał kartę?
   b) Kto jest posiadaczem karty?
   c) Jaki jest cel użycia karty?
   d) Czy osoba ta posiada wiele kart i dlaczego?
   e) Czy jest w pobliżu urządzenia zdolne do sczytywania kart?

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:

1. Numery zabezpieczanej karty.
2. Dane o właścicielu karty.

3. Historia transakcji.
4. Dane dystrybutora karty.
5. Czas i miejsce wydania.
6. Termin ważności karty.

ID Card Printer jest specjalistycznym rodzajem drukarki, umożliwiającej wydrukowanie w pełni funkcjonalnej karty magnetycznej.

Procedura zabezpieczania ID Card Printer'a:

1. W pierwszej kolejności należy ocenić, czy ma się do czynienia z wersją drukarki podłączonej do innego urządzenia lub sieci cyfrowej, stacjonarną czy przenośną.
2. Jeżeli urządzenie jest włączone, nie należy go wyłączać – może to spowodować utratę danych zawartych w pamięci o ostatnich wykonywanych przez drukarkę czynnościach.
3. Jeżeli drukarka jest w trakcie pracy, należy pozwolić jej dokończyć drukowanie.
4. W przypadku, gdy sprzęt jest podłączony i operowany przez komputer, należy sprawdzić, czy w pamięci komputera nie zostały zaplanowane druki nowych kart.
5. Większość sprzętów tego typu posiada gniazda USB na pamięć przenośną – podobnie jak w przypadku opisywanego wcześniej telefaksu, należy podjąć próbę skopiowania pamięci tymczasowej na nośnik zewnętrzny, np. pendrive.
6. W przypadku, gdy na miejscu zabezpieczania nie ma eksperta z zakresu informatyki, nikt z osób obecnych nie jest w posiadaniu dysków przenośnych i drukarka jest włączona, trzeba poprzestać na zabezpieczeniu pomieszczenia przed osobami trzecimi, odłączeniu sieci cyfrowej i wstrzymaniu dalszych czynności z drukarką do czasu przybycia eksperta.
7. Należy przeszukać pomieszczenie i zabezpieczyć wszystkie dokumenty i instrukcje mające związek z drukarką.
8. W przypadku wyłączonego urządzenia należy je odłączyć i szczegółowo opisać każdy z zabezpieczanych elementów, sfotografować sprzęt i zapakować do pojemników na czas podróży.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:

1. Plany druku kart magnetycznych.
2. Historia drukowania.
3. Daty i godziny druku.
4. Materiały, na jakich dokonywany jest druk.

Drukarka jest obecnie najpowszechniej występującym sprzętem biurowym i domowym, służącym do pracy z komputerem. Urządzenie pozwala drukować materiały na kartkach papieru w wielu formatach. Część z drukarek jest wyposażona w funkcję skanera, faksu, możliwość łączenia się z siecią internetową i telefoniczną. Nowocześniejsze drukarki są wyposażone we własną przestrzeń

pamięci, a także złącza USB, pozwalające na drukowanie z pamięci przenośnej. Rozróżniamy drukarki tuszowe i laserowe.

Procedura zabezpieczania drukarki komputerowej:

1. Jeżeli drukarka jest wyłączona, należy dokładnie ją sfotografować i opisać. Trzeba sprawdzić, czy jest podłączona do komputera. Następnie trzeba odłączyć drukarkę od zasilania, Internetu i sieci telefonicznej, jeżeli posiada takie podłączenia, spisując numery telefonów i sieci, za pomocą których jest podłączona.
2. W przypadku, gdy drukarka pozostała włączona, pochopne wyłączenie jej spowoduje utratę potencjalnie istotnych danych cyfrowych z ostatnich godzin pracy sprzętu. Należy pozostawić ją włączoną.
3. Jeżeli jest taka możliwość, trzeba użyć dysku przenośnego w celu zabezpieczenia danych tymczasowych. Jeżeli nie ma takiej możliwości, trzeba zaczekać na przybycie eksperta z zakresu informatyki.
4. Włączoną drukarkę należy odizolować od osób trzecich do czasu przybycia eksperta.
5. Jeżeli sprzęt jest w trakcie druku, nie powinno się przerywać tego procesu.
6. W przypadku wyłączonej drukarki można ją zapakować do pojemnika w celu przetransportowania do analizy.
7. Zabezpieczone powinny pozostać wszystkie odnalezione dokumenty i elementy związane z drukarką.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:

1. Dane dotyczące ostatnio drukowanych dokumentów.
2. Pamięć zawierającą daty i godziny.
3. Pliki przechowywane w pamięci drukarki przeznaczone do wielokrotnego druku.
4. Numery telefoniczne, z którymi urządzenie jest powiązane.

Skaner jest urządzeniem powszechnie wykorzystywanym w domach i biurach. Sprzęt umożliwia zeskanowanie materiałów do formatów cyfrowych, takich jak pliki graficzne. Wiele ze współczesnych skanerów posiada funkcję przechowywania pewnej części zeskanowanych dokumentów w pamięci podręcznej. Istnieją różne typy skanerów, począwszy od najbardziej rozpowszechnionych skanerów stacjonarnych. Kolejnym rodzajem są skanery wbudowane w inne urządzenia, np. kserokopiarki i występują także skanery przenośne, pozwalające na szybkie zeskanowanie do pamięci urządzenia powierzchni, po której zostaną przeciągnięte. Skanery przenośne zapewniły sobie stałe miejsce w gronie urządzeń specjalistycznych, a nawet szpiegowskich. Dzięki nim możliwe jest zrobienie szybkiej kopii wybranego dokumentu.

Procedura zabezpieczania skanera:

1. W przypadku wyłączonego urządzenia należy sprawdzić, czy jest ono podłączone do komputera i sieci cyfrowej lub telefonicznej. Po odłączeniu wszystkich kabli można przystąpić do dalszych kroków.

2. Należy szczegółowo opisać zabezpieczane urządzenie, dodając materiał fotograficzny. Następnie zapakować urządzenie do szczelnych pojemników na czas transportu do specjalistycznej analizy.
3. W przypadku włączonego urządzenia pod żadnym pozorem nie wolno go wyłączyć. Może to spowodować utratę przechowywanych danych w pamięci podręcznej.
4. Jeżeli istnieje taka możliwość, należy użyć dysku przenośnego, np. pendrive (większość skanerów posiada wbudowane złącza USB) i dokonać próby zgrania pamięci zawartej na dysku skanera.
5. W przypadku, gdy brak jest odpowiednich środków do przekopiowania pamięci, należy odizolować urządzenie od osób trzecich i pozostawić całość do czasu przybycia eksperta z zakresu informatyki.
6. Jeżeli skaner jest w trakcie pracy, trzeba pozwolić urządzeniu dokończyć operację. Przerwanie procesu skanowania może zniekształcić tworzony obraz graficzny kopiowanego materiału do stopnia całkowicie nieczytelnego.
7. W miarę możliwości należy zabezpieczyć też wszystkie odnalezione dokumenty powiązane z urządzeniem, a także materiały umieszczone na czytniku urządzenia, będące w przygotowaniu do skanowania lub po procesie skanowania.
8. Całość materiału powinna być umieszczona w bezpiecznym pojemniku, chroniącym urządzenie przed zniszczeniem i wpływem czynników szkodliwych.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:

1. Dane zawarte w pamięci urządzenia na temat ostatnich wykonanych operacji.
2. Kopie cyfrowe zeskanowanych plików.
3. Daty i godziny.

Kopiarki są obecne praktycznie we wszystkich biurach i urzędach. W odróżnieniu od skanerów i drukarek, łączą w sobie funkcję różnych maszyn, a ich przeznaczeniem jest praca w znacznie większym wymiarze niż wcześniej opisywane urządzenia. Kopiarki są dostosowane do wydajnej pracy z dużą ilością materiału. Duża część z takich urządzeń posiada również funkcję faksu, połączenie z siecią internetową, połączenie z siecią komputerową, umożliwiającą zdalne przesyłanie żądań wykonania wybranych operacji nawet przez wiele komputerów równocześnie. Kopiarki posiadają też znaczną ilość wbudowanej pamięci dla przechowywanych danych i gniazda USB dla pamięci zewnętrznej.

Procedura zabezpieczania kopiarki:

1. W przypadku wyłączonego urządzenia należy je dokładnie opisać i sfotografować. Następnie odłączyć wszelkie źródła zasilania i kable sieciowe. Całość ze względu na swoje gabarytu powinna być zabezpieczona w sposób umożliwiający późniejszą analizę.
2. Jeżeli kopiarka jest włączona, bardzo ważne jest, by nie wyłączać urządzenia. Pochopne odcięcie źródła zasilania spowoduje utratę danych na temat ostatniej wykonywanej czynności na urządzeniu lub operacji, jaka była wykonywana.

3. W miarę możliwości należy skopiować zawartość dysku kopiarki na pamięć przenośną. Jeżeli nie można tego dokonać, wymagana jest obecność eksperta z zakresu informatyki.
4. Należy przeszukać otoczenie i zabezpieczyć wszystkie możliwe dokumenty związane z kopiarką, zwłaszcza zwracając uwagę na instrukcję obsługi. Kopiarki bywają często skomplikowane w użytkowaniu i posiadają wiele skomplikowanych funkcji.
5. Jeżeli kopiarka była zsynchronizowana z więcej niż jednym komputerem, należy sprawdzić, czy w ostatnim czasie były wysyłane z komputerów jakieś żądania.
6. W przypadku, gdy kopiarka jest podłączona do sieci telefonicznej, należy sprawdzić i spisać numer telefoniczny, przez który odbywały się połączenia.
7. Urządzenie należy odizolować od osób trzecich.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:

1. Pliki zapisane w pamięci urządzenia, zapisane kopie.
2. Ostatnie przeprowadzone operacje.
3. Numery telefoniczne w przypadku funkcji faksu.
4. Dane dotyczące ilości i rodzaju zsynchronizowanych urządzeń z daną kopiarką.
5. Daty i godziny.
6. Listy połączeń przychodzących i wychodzących.

Płyty CD i DVD są najpowszechniej wykorzystywanymi środkami przechowywania danych cyfrowych na nośnikach przenośnych. Płyty CD posiadają obszar pamięci do 700 MB, natomiast płyty DVD obszar do 4,7 GB (4,700 MB). Nośnik taki stanowi kawałek plastiku ze specjalną powierzchnią umożliwiającą laserowe nanoszenie danych, które później mogą zostać odczytane na dowolnej maszynie wyposażonej w odpowiedni czytnik lub oprogramowanie. Inne rodzaje pamięci przenośnej składają się na rodziny dysków przenośnych, do których należą wszelkiej maści pendrive'y, dyski USB, karty pamięci SD, MicroSD i inne. Najczęstszymi przypadkami zabezpieczania tego typu nośników są sprawy związane z łamaniem praw autorskich lub przechowywaniem treści zabronionych, jak np. zdjęcia i filmy o charakterze pedofilskim. Przedstawiany rodzaj pamięci jest używany przez każdą osobę będącą w styczności z komputerami.

Procedury zabezpieczania płyt kompaktowych i pamięci przenośnej:

1. Po odnalezieniu dysku przenośnego powinno się go natychmiast zabezpieczyć w odpowiednim pojemniku, chroniącym przed osobami trzecimi i zniszczeniem.
2. Nie należy uruchamiać, odczytywać i zapisywać nowych danych na odnalezionych nośnikach. Część z dysków przenośnych może funkcjonować w odmiennych formatach plików, np. FAT32, NTFS, exFAT itp. W niektórych przypadkach podłączenie dysku do komputera bez odpowiedniej znajomości jego

struktury może spowodować utratę wszystkich danych zawartych w pamięci urządzenia, np. dyski z urządzeń monitorujących.
3. W przypadku, gdy odnaleziona pamięć przenośna jest podłączona do komputera, należy zamknąć proces w systemie i odłączyć urządzenie.
4. Jeżeli komputer jest w trakcie pracy i trwa kopiowanie nowych danych na podłączony nośnik, nie należy przerywać operacji.

Potencjalne dane, mogące stanowić dowody, jakie mogą być odnalezione:
1. Wszelkie pliki audio/video i tekstowe zawarte w pamięci urządzenia.
2. Daty i godziny.
3. Historia pracy urządzenia.

Wykorzystywane powszechnie urządzenia odbierające materiały audio i video pozwalają każdemu na utrwalanie teraźniejszości pod postacią multimedialnych plików cyfrowych. Większość urządzeń tego rodzaju jest wyposażona w pamięć pozwalającą przechowywać pewną ilość zarejestrowanych plików. Pamięć taką można rozszerzać poprzez dodawanie zewnętrznych kart pamięci, np. SD lub MicroSD. Część kamer i aparatów posiada także wejścia USB i MicroUSB umożliwiające podłączanie do komputerów, telewizorów itp. Nowoczesne modele posiadają funkcję sieciowe i są w stanie przesyłać przechowywane materiały za pomocą sieci bezprzewodowej.

Procedura zabezpieczania cyfrowych kamer aparatów fotograficznych:
1. Jeżeli urządzenie jest wyłączone, nie wolno go włączać – może to spowodować nadpisanie istotnych materiałów cyfrowych.
2. W przypadku, gdy urządzenie jest włączone, należy w miarę możliwości przestawić tryb pracy sprzętu na niski pobór energii i nie dopuścić, by całkowicie rozładowana została bateria. Wiele z obecnie występujących kamer i aparatów posiadają wbudowane akumulatory energii, które można zasilać poprzez USB.
3. Jeżeli ekspert nie jest dostępny, trzeba jak najszybciej zabezpieczyć, zidentyfikować i opisać rodzaj materiałów audio/video.
4. Natychmiast trzeba zabezpieczyć istniejące materiały audio i video, by nie zostały nadpisane.
5. Pewne modele aparatów wykorzystują klisze filmowe – wysoce zalecane jest, by nie wyjmować filmu z kasety urządzenia przed jej wyczerpaniem i bez odpowiedniego przygotowania.
6. Całe urządzenie należy sfotografować i opisać, wliczając w to stan wyświetlacza. Jeżeli jest podłączone do innego źródła, np. komputera, trzeba sprawdzić, jakie pliki zostały przeniesione z pamięci podręcznej i odłączyć kabel wykorzystany przy połączeniu.
7. Zabezpieczyć materiał dowodowy, taki jak klisze filmowe, do szczelnego pojemnika uniemożliwiającego ingerencję osoby trzeciej.
8. Poza sprzętem głównym, należy zabezpieczyć całe okablowanie i wszystkie komponenty dodatkowe, np. dokumenty, instrukcje obsługi, pokrowce.

9. Z uwagi na delikatną naturę sprzętu, jakim są kamery i aparaty, w przypadku konieczności przetransportowania do specjalistycznego laboratorium informatycznego trzeba dochować wszelkich starań, by pojemniki do przechowywania były odporne na czynniki zewnętrzne.
10. Całość trzeba jak najszybciej dostarczyć do badań przez eksperta. Jeżeli zajdą opóźnienia, może dojść do wyczerpania się energii zasilającej urządzenia i w konsekwencji do bezpowrotnej utraty części danych z pamięci dysku.

Potencjalne dane, mogące stanowić dowody, jakie mogą zostać odnalezione:

1. Pliki audio/video.
2. Wiadomości tekstowe.
3. Daty i godziny.
4. Historia połączeń multimedialnych i sieciowych.
5. Pliki tekstowe.
6. Inne istotne elementy.

Współczesne konsole multimedialne są urządzeniami służącymi rozrywce. Sprzęt jest wyposażony w funkcję konsoli do gier, odtwarzacza płyt DVD i BlueRay; pozwalają na łączenie się z siecią cyfrową i są także wyposażony w przestronny dysk pamięci podręcznej HDD. Głównymi celami zabezpieczania tego typu urządzeń są konsekwencje wynikające z łamania praw autorskich i piractwa na szeroką skalę. Dotyczy to głównie technicznego przerabiania konsoli na zdolną do odtwarzania pirackiego oprogramowania i płyt. Zanosząc sprzęt do odpowiedniego specjalisty i dokonując odpowiedniej opłaty, odbieramy urządzenie będące w stanie np. ominąć zabezpieczenia wynikające z nakładanych systemów PAL i NTSC, a także zyskujemy inne przywileje kosztem złamania prawa. Dodatkowo na dysku urządzenia mogą być przechowywane dowolne treści audio/video, także takie o charakterze pedofilskim. Rozróżniamy dwa rodzaje konsol multimedialnych – są nimi konsole stacjonarne i przenośne. Różnica polega na wielkości urządzenia, mocy obliczeniowej i możliwościach cyfrowych.

Procedura zabezpieczania konsoli multimedialnych:

1. Jeżeli urządzenie jest wyłączone, nie należy go włączać. Podobnie jak w przypadku innych sprzętów cyfrowych opisywanych wcześniej, tak i tutaj może nastąpić utrata pewnych danych cyfrowych.
2. Należy sprawdzić, czy konsola jest podłączona do sieci cyfrowej i elektrycznej.
3. W przypadku stwierdzenia istnienia połączenia cyfrowego należy je natychmiast odłączyć, by zapobiec potencjalnemu nadpisaniu danych, np. poprzez automatyczną aktualizację systemową.
4. Całość należy szczegółowo opisać i sfotografować, dodając również wykres przedstawiający sposób połączenia sprzętu. Niektórzy wykorzystują konsolę w innych celach – jako bazę. Osoba zaznajomiona ze specjalistyczną wiedzą może wykorzystać konsolę posiadającą dużą moc obliczeniową do innych celów.

5. Trzeba sprawdzić czytnik urządzenia, w którym może znajdować się źródło pamięci przenośnej, np. płyta CD lub dyski UMD itp.
6. W przypadku, gdy konsola jest włączona, należy skontaktować się z ekspertem.
7. Należy opisać i sfotografować stan wyświetlacza lub ekranu monitora czy telewizora.
8. W przypadku konieczności przetransportowania sprzętu do laboratorium kryminalistycznego całość należy odpowiednio zabezpieczyć w pojemnikach transportowych, koniecznie unikając czynników mogących doprowadzić do zniszczenia lub uszkodzenia urządzeń cyfrowych, np. silne pole magnetyczne, wysoka i niska temperatura itp.
9. Jeżeli są dostępne dokumenty odnoszące się do zabezpieczanego sprzętu, np. instrukcja obsługi czy specyfikacja techniczna, należy dostarczyć je wraz ze sprzętem do odpowiedniego eksperta.

Potencjalne dane, mogące stanowić dowody, jakie mogą zostać odnalezione:

1. Dane zawarte w pamięci urządzenia.
2. Daty i godziny.
3. Materiał audio/video.
4. Pirackie oprogramowanie.
5. Dodatkowe komponenty elektroniczne (chipy, procesory itp.).

Urządzeniami zaliczanymi do sprzętów gospodarstwa domowego są wszelkie maszyny popularnie wykorzystywane w domostwach obywateli, jak np. telewizory, lodówki, mikrofalówka, pralki itp. Współczesne sprzęty tej kategorii są wyposażone w zaawansowane opcje dodatkowe. Dzięki bogatym funkcjom można sprawdzić na lodówce temperaturę, jaka panuje wewnątrz, połączyć się z siecią internetową, telewizory dokonują aktualizacji, pobierają filmy na wewnętrzny dysk telewizora z usługi wypożyczalni filmów itp. Większość takich urządzeń posiada możliwość łączenia się z siecią cyfrową lub teleinformatyczną, stając się elementami w sieci cyfrowej. Sprzęty gospodarstwa domowego nie różnią się w dużym stopniu od tradycyjnego komputera, posiadają dyski, procesory i podstawowe funkcje systemowe. W świetle niedawnych wydarzeń, jakimi było zlokalizowanie groźnej sieci botnet, wykorzystującej w celach rozsyłania spamu komputerowego (niechciane wiadomości zawierające nachalne reklamy lub wirusy) – tysiące sprzętów gospodarstwa domowego, np. lodówek i telewizorów zostało tym wirusem „zainfekowanych". Hakerzy wykorzystali funkcje komputerowe i połączenia z Internetem sprzętów gospodarstwa domowego do własnych celów. O ataku jako pierwsza doniosła firma Proofpoint – w skład zakażonych złośliwym oprogramowaniem sprzętów weszło około 100 tysięcy urządzeń[229].

[229] K. Dzieliński: *Hakerski atak z pomocą lodówki*, http://www.geekweek.pl/aktualnosci/18338/hakerski-atak-z-pomoca-lodowki.

Procedura zabezpieczania „home electronic devices":

1. W przypadku, gdy zabezpieczane urządzenie jest wyłączone, nie należy go włączać – może to spowodować nadpisanie istniejących danych w pamięci.
2. Jeżeli urządzenie jest włączone, należy skontaktować się z odpowiednim ekspertem.
3. W przypadku, gdy ekspert jest niedostępny, można podjąć pewne czynności w celu zabezpieczenia sprzętu. W pierwszej kolejności należy sfotografować całość zabezpieczanego urządzenia, uwzględniając ekran wyświetlacza (jeżeli sprzęt takowym dysponuje) i sposób podłączenia okablowania.
4. Jeżeli urządzenie pozwala na odtwarzanie zapisanych plików audio, należy odtworzyć zawartość, zgrywając jej treść. Niektóre sprzęty gospodarstwa domowego pozwalają na zostawianie wiadomości głosowych, np. dla innych domowników lub użytkowników.
5. W następnej kolejności trzeba odłączyć wszelkie źródła zasilania od zabezpieczanego urządzenia.
6. Należy umieścić taśmę zabezpieczającą lub plomby na wszystkich możliwych otworach cyfrowych i wejściach umożliwiających wprowadzanie nośników pamięci.
7. Poza zabezpieczeniem samego urządzenia, należy również zabezpieczyć okablowanie i komponenty dodatkowe, np. zasilacz itp.
8. W przypadku, gdy konieczny jest transport, urządzenia należy odpowiednio zabezpieczyć, zapakować w pojemnik chroniący przed czynnikami zewnętrznymi i osobami trzecimi. Sprzęt elektroniczny jest szczególnie wrażliwy na oddziaływanie silnego pola magnetycznego, bardzo niskie i wysokie temperatury.
9. W przypadku, gdy źródłem zasilania zabezpieczanego sprzętu jest bateria, należy dołożyć wszelkich starań, by nie została ona rozładowana. Utrata zasilania z podobnego źródła może spowodować nieodwracalną utratę części danych zawarty w pamięci masowej.
10. Jeżeli jest taka możliwość, należy odnaleźć wszystkie przydatne dokumenty związane z urządzeniem i dołożyć je do zabezpieczanego sprzętu, np. instrukcje obsługi, dokumenty dotyczące zakupu, gwarancje itp.
11. Często w przypadkach zabezpieczania sprzętu należącego do grupy „gospodarstwa domowego" wymagane będzie skontaktowanie się z firmą produkującą dany typ urządzenia i uzyskanie dodatkowych informacji o charakterze specjalistycznym i techniczno-informatycznym.

Potencjalne dane, mogące stanowić dowody, jakie mogą zostać odnalezione:

1. Dane zawarte w pamięci urządzenia – zdjęcia, pliki audio/video, pliki tekstowe itp.
2. Dane dostępowe do sieci internetowej.
3. Historia połączeń cyfrowych.

4. Historia wysyłanych i otrzymywanych danych przez sieć teleinformatyczną.
5. Dane telefoniczne i historię połączeń telefonicznych.
6. Podstawowe wykonywane funkcje systemowe.
7. Źródło nadawanego sygnału (może być częścią zabezpieczonego urządzenia lub stanowić odrębną bazę będącą samodzielnym sprzętem cyfrowym).

GPS staje się standardem na wyposażeniu współczesnych urządzeń cyfrowych. Nawigacja satelitarna nie jest już luksusem przeznaczonym dla kierowców samochodowych. Obecnie wszystkie telefony posiadają aplikację i funkcję pozwalającą korzystać z dobrodziejstw technologii inteligentnej nawigacji. Sam system GPS ma na celu ułatwienie podróży, wskazanie najkrótszej drogi do celu lub przedstawienie okolicy danemu użytkownikowi. Ustalenie pozycji urządzenia odbywa się za pomocą licznej sieci przekaźników ulokowanych na terenie całego świata, które łączą się z satelitami znajdującymi się na orbicie okołoziemskiej. Systemy GPS są w stanie określić dokładną pozycję użytkownika na świecie z dokładnością do 2 metrów. Występują różne typy urządzeń z rodzaju GPS. Istnieją modele stacjonarne, przenośne lub będące częścią składową innych urządzeń teleinformatycznych, np. telefonów komórkowych. System GPS jest obecnie bardzo mocno eksploatowany i wykorzystywany w większości dziedzin życia społecznego i gospodarczego.

Procedura zabezpieczania GPS:

1. Jeżeli urządzenie jest wyłączone, nie należy go włączać. Może to spowodować utratę części danych zawartych w pamięci urządzenia.
2. W przypadku, gdy sprzęt GPS jest włączony, należy skontaktować się z ekspertem.
3. Jeżeli ekspert nie jest dostępny, można dokonać kilku czynności w celu optymalnego zabezpieczenia danego urządzenia.
4. Należy opisać i sfotografować ekran urządzenia, jak i samo urządzenie, uwzględniając również wszelkie połączenia kabli. Dla ułatwienia można utworzyć diagram przedstawiający system połączeń.
5. Trzeba odłączyć wszelkie źródła zasilania, np. kable, odłączając je od tylnej strony urządzenia.
6. Należy umieścić taśmę zabezpieczającą lub plomby na wszystkich możliwych otworach cyfrowych i wejściach umożliwiających wprowadzanie nośników pamięci.
7. Zabezpieczyć wszystkie dodatkowe komponenty, takie jak okablowanie, dokumenty itp.
8. W przypadku, gdy niezbędne będzie przetransportowanie urządzenia, należy je zabezpieczyć w odpowiednim pojemniku chroniącym od czynników zewnętrznych (pole magnetyczne, niska i wysoka temperatura), a także potencjalnej ingerencji osób nieupoważnionych.
9. Jeżeli urządzenie jest włączone i zasilane baterią, nie można dopuścić do rozładowania się energii urządzenia. Utrata stałego źródła zasilania będzie miała

inny efekt niż w przypadku odcięcia dopływu prądu przez kabel elektryczny, może wyrządzić nieodwracalne straty w pamięci urządzenia i zawartych tam danych cyfrowych.
10. W przypadku, gdy istnieje taka możliwość, należy zgrać zawartość pamięci urządzenia na dysk zewnętrzny.
11. Należy uzyskać wszystkie dane wymagane do autoryzacji użytkownika urządzenia, takich jak hasła i loginy, a także wszystkie możliwe do uzyskania informacje dodatkowe posiadające istotne znaczenie.
12. W przypadku zabezpieczania urządzeń z grupy GPS, wymagane będzie skontaktowanie się z producentem w celu ustalenia szczegółowych informacji techniczno-informatycznych.
13. Jeżeli GPS jest częścią innego urządzenia, np. komputera lub telefonu, należy zabezpieczyć go zgodnie z procedurami odpowiednimi dla danego urządzenia.

Potencjalne dane, mogące stanowić dowody, jakie mogą zostać odnalezione:
1. Dane zawarte w pamięci urządzenia – pliki tekstowe, mapy i obrazy cyfrowe.
2. Dane połączeń internetowych.
3. Połączenia radiowe wychodzące i przychodzące.
4. Dane telefoniczne (w przypadku, gdy urządzenie GPS posiada taką funkcję).
5. Historię połączeń teleinformatycznych.
6. Dane routera i zapamiętane lokacje na mapie.
7. Historię odwiedzonych miejsc i przebytych tras.
8. Daty i godziny.

PDA jest to „komputer kieszonkowy" posiadający funkcję komputera, ale będący od niego znacznie mniejszy. Różnica pomiędzy PDA a komputerami stacjonarnymi i przenośnymi polega także na znacznie mniejszej mocy obliczeniowej, jaką dysponuje PDA. Komputery kieszonkowe to urządzenia wielofunkcyjne, zdolne do odbierania, wysyłania, przechowywania i przetwarzania danych cyfrowych, takich jak pliki audio/video, tekstowe, obrazy itp. W dzisiejszych czasach PDA uchodzą już za urządzenia przestarzałe, większość ich funkcji i zalet została przejęta przez zaawansowanie techniczne telefony komórkowe i tablety. Mimo powszechnego zacofania technicznego względem konkurencyjnych urządzeń, PDA nadal są powszechnie używane.

Procedura zabezpieczania PDA – Personal Data Assistants (palmtop):
1. Jeżeli PDA jest wyłączone, nie wolno go uruchamiać. Tak jak w przypadku większości urządzeń cyfrowych, taki zabieg może spowodować nadpisanie lub utratę części danych znajdujących się w pamięci urządzenia.
2. W przypadku, gdy PDA jest włączone, trzeba skontaktować się z ekspertem.
3. Gdy ekspert nie jest dostępny, należy wykonać następujące czynności w celu zabezpieczenia urządzenia.
4. Szczegółowo opisać i sfotografować urządzenie, uwzględniając stan wyświetlacza i sposób podłączenia dodatkowych komponentów.

5. Odłączyć źródło zasilania stacjonarnego, np. kabel od prądu, nie wolno wyjmować baterii wewnętrznej PDA.
6. Należy umieścić taśmę zabezpieczającą lub plomby na wszystkich możliwych otworach cyfrowych i wejściach umożliwiających wprowadzanie nośników pamięci.
7. Sporządzić diagram przedstawiający sposób podłączenia urządzenia do innych sprzętów cyfrowych, jeżeli takowe są podłączone.
8. W razie konieczności przetransportowania sprzętu w celach analizy, należy zabezpieczyć urządzenie w odpowiednim pojemniku chroniącym od czynników zewnętrznych i osób trzecich.
9. Jeżeli urządzenie jest zasilane przez baterię, nie można dopuścić do rozładowania się źródła zasilania. Zaniedbanie takie może doprowadzić do bezpowrotnej utraty części danych zawartych w pamięci PDA.
10. Poza samym PDA, należy zabezpieczyć wszelkie komponenty dodatkowe, takie jak: rysik cyfrowy, dokumenty, instrukcje obsługi, kable zasilające i przesyłowe.
11. W celu uzyskania dostępu do danych systemowych zawartych w pamięci może zaistnieć konieczność skontaktowania się z producentem danego urządzenia.

Potencjalne dane, mogące stanowić dowody, jakie mogą zostać odnalezione:

1. Dane zawarte w pamięci PDA, np. pliki audio/video, dokumenty tekstowe, obrazy cyfrowe itp.
2. Dane dotyczące połączenia internetowego.
3. Historię połączeń z siecią cyfrową.
4. E-maile i inne wiadomości tekstowe.
5. Lokalizacje.
6. Daty i godziny.
7. Podstawowe dane zawarte w systemie.
8. Urządzenie może być samodzielne lub stanowić część sieci teleinformatycznej – powiązania sieciowe.
9. Zasięg poprawnego funkcjonowania sieci, w jakiej pracuje urządzenie.

Systemy bezpieczeństwa cyfrowego są to zestawy urządzeń funkcjonujących we wspólnej sieci teleinformatycznej, zapewniające ochronę danym obiektom lub miejscom. Do grupy takich urządzeń należą najczęściej alarmy domowe, kamery monitorujące, sieci bezpieczeństwa miast. System składa się najczęściej z kilku elementów, których wspólną cechą jest baza główna, do której przesyłane są zbierane informacje i tam magazynowane pod postacią danych cyfrowych.

Procedura zabezpieczania systemów bezpieczeństwa cyfrowego – security systems:

1. W każdym przypadku wymagana jest specjalistyczna wiedza z zakresu informatyki.

2. Zabezpieczyć miejsce, w którym znajduje się baza systemu od osób postronnych.
3. Jak najszybciej odłączyć dyski pamięci w celu zabezpieczenia ich przed możliwym nadpisaniem danych zawartych w pamięci.
4. Przed przybyciem eksperta, w celu ułatwienia i przyśpieszenia procesu zabezpieczania, należy ustalić następujące informacje: model urządzenia, producent, system operacyjny, system i formaty obsługiwanego video i audio, liczba kamer i mikrofonów, typ kamer, lokalizacja wszystkich dodatkowych elementów systemu bezpieczeństwa, miejsce przechowywania pamięci urządzenia, lokalizacja archiwum.
5. Należy dokładnie sfotografować stan bazy urządzenia i wykonać diagram przedstawiający system bezpieczeństwa z uwzględnieniem kamer i innych elementów.
6. Ustalić wszelkie potrzebne dane do autoryzacji w systemie od pracowników obsługujących dane urządzenie.
7. Skontaktować się z producentem systemu i sprzętu, jeżeli zajdzie potrzeba uzyskania dodatkowych danych istotnych dla poprawnego przebiegu procesu analizy.
8. Po przybyciu specjalisty wszelkie czynności analizy informatyczno-kryminalistycznej należy wykonywać w miejscu odnalezienia bazy systemu.
9. Jeżeli zachodzi konieczność przetransportowania systemu bezpieczeństwa do laboratorium kryminalistycznego, koniecznie należy zabezpieczyć całość bazy głównej. Zabezpieczenie samych nośników pamięci (dysków) i próba ich analizy na zwykłym komputerze stacjonarnym może spowodować całkowite ich wykasowanie przez różnice wynikające z systemów, w jakich pracują urządzenia systemu bezpieczeństwa a komputerami stacjonarnymi. Wymagane jest używanie w celach analizy dokładnie takich samych systemów, w jakich pracują zabezpieczone nośniki.
10. Całość należy dokładnie zabezpieczyć w odpowiednie pojemniki chroniące od czynników zewnętrznych i osób trzecich.

Potencjalne dane, mogące stanowić dowody, jakie mogą zostać odnalezione:

1. Dane zawarte w pamięci urządzenia, np. pliki audio/video, dokumenty tekstowe, obrazy cyfrowe itp. Dane te mogą stanowić także przedmiot badań innych biegłych w zakresie identyfikacji osób na podstawie nagrania[230].
2. Czas nagrania.
3. System może być samodzielny lub stanowić część większej sieci – dane zarejestrowane przez urządzenia peryferyjne.
4. Daty i godziny.

---

[230] Por. P. Waszkiewicz: *Wielki Brat Rok 2010. Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne,* Warszawa 2011, s. 177 i nast.

Wszystkie współczesne samochody są wyposażone w pokładowe komputery umożliwiające rozszerzenie funkcji i polepszenie komfortu użytkownika. Urządzenia są wyposażone w systemy operacyjne zawierające podstawowe funkcje zwykłych komputerów, posiadają dyski pamięci, na których przechowywane są określone dane cyfrowe. Serwisy samochodowe rejestrują w sprzęcie tego typu historię przeglądów, datę sprzedaży, właściciela itp.

Procedura zabezpieczania komputerów pokładowych:

1. W przypadku, gdy urządzenie jest wyłączone, nie należy go włączać. Podobnie jak w przypadku wcześniej opisywanych urządzeń cyfrowych, uruchomienie systemu może nadpisać lub usunąć niektóre dane zawarte w pamięci.
2. Jeżeli sprzęt jest włączony, należy skontaktować się z ekspertem.
3. W pierwszej kolejności należy szczegółowo opisać i sfotografować ekran wyświetlacza, uwzględniając wszystkie zaobserwowane informacje. Należy również zwrócić uwagę na markę samochodu i rodzaj komputera pokładowego.
4. Z uwagi na specyficzne umieszczenie komputera pokładowego jako najczęściej stałego elementu deski rozdzielczej może być niemożliwe jego odłączenie. Inaczej sprawa może wyglądać, jeżeli chodzi o dyski pamięci wykorzystywane przez komputer. Dyski takie są najczęściej możliwe do zdemontowania – należy zapoznać się z dokładną instrukcją modelu pojazdu, na którym dokonywana jest analiza w celu ustalenia przybliżonej lokalizacji pamięci cyfrowej. Po odnalezieniu dysku należy go odłączyć od komputera pokładowego.
5. Umieścić taśmę zabezpieczającą i plomby na wszystkie wejścia cyfrowe komputera pokładowego i zabezpieczonych dysków pamięci.
6. Podczas odłączania pamięci cyfrowej wskazane jest sporządzenie diagramu przedstawiającego sposób podłączania sprzętu i dodatkowo należy sfotografować sposób jego podłączenia.
7. Zabezpieczyć wszystkie dodatkowe komponenty i kable.
8. W przypadku występowania zasilania za pomocą baterii, należy dochować wszelkich starań w celu niedopuszczenia do rozładowania baterii. Ewentualnie całkowite wyładowanie się źródła zasilania może spowodować utratę cennych informacji zawartych pod postacią cyfrową.
9. Jeżeli zachodzi konieczność przetransportowania zabezpieczonych urządzeń w celach późniejszej analizy, należy je odpowiednio zabezpieczyć za pomocą specjalistycznych pojemników chroniących od nadmiernej temperatury lub zbyt niskiej i innych negatywnych czynników.
10. Zabezpieczyć wszelkie instrukcje obsługi, dokumenty związane z korzystaniem z pojazdu, materiały związane z obsługą komputera pokładowego.
11. Skontaktować się z producentem danego rodzaju pojazdu lub komputera pokładowego w celu uzyskania specjalistycznych informacji mogących znacznie ułatwić pracę i analizę na zabezpieczonych urządzenia.

12. System zawarty w komputerze pokładowym może być kompatybilny z wieloma innymi rodzajami systemów: komunikacyjnym, nawigacyjnym, bezpieczeństwa, ochrony danych, rozrywkowym, osobistym, internetowym, muzycznym, domowym z możliwością zdalnego łączenia się, roboczym, pracodawcy, publicznym (usługi reklamowe) i systemem urządzeń przenośnych (telefony, tablety, komputery, pendrive, PDA itp.), dlatego może zajść konieczność pozyskania większej liczby informacji o celu poszukiwań i rodzaju danych wymaganych do wyśledzenia.

Potencjalne dane, mogące stanowić dowody, jakie mogą zostać odnalezione:

1. Dane zawarte w pamięci urządzenia, np. pliki audio/video, dokumenty tekstowe, obrazy cyfrowe itp.
2. Dane dostępowe do sieci internetowej.
3. Historia połączeń telefonicznych w przypadku wykorzystywania funkcji połączeń za pomocą sieci teleinformatycznej.
4. Lokalizacje logowań routera i nadajnika GPS.
5. Daty i godziny.
6. Dane systemowe przebiegu i zużycia pojazdu.
7. Wiadomości i poczta mailowa.

Nowoczesne technologie pozwalają przestępcom na wykorzystywanie bardzo wyrafinowanych metod popełniania czynów zabronionych z wykorzystaniem urządzeń cyfrowym. Do grupy urządzeń określanych jako „technologie przestępcze" możemy zaliczyć np. nielegalne i nieautoryzowane czytniki kart magnetycznych, skanery kodów i banknotów, pluskwy, podsłuchy, keyloggery i inne urządzenia cyfrowe wykorzystywane w złej wierze. Najczęściej są to urządzenia będące nielegalnie podłączonymi i funkcjonującymi, na zasadzie „pasożyta", pod większe sprzęty cyfrowe. Można tutaj wyróżnić fałszywe czytniki kart bankowych montowane w bankomatach przez złodziei. Urządzenia z grupy przestępczych charakteryzują się najczęściej niewielkim rozmiarem, konstrukcją sprecyzowaną na wykonywanie ściśle określonych celów. Urządzenia takie posiadają zawsze pamięć masową, w której przechowywane są skradzione dane lub nadajnik umożliwiający natychmiastowe wysyłanie przechwytywanych informacji wprost do komputera hakera.

Procedura zabezpieczania skanerów, czytników, pluskw i innych przestępczych urządzeń:

1. Jeżeli urządzenie jest wyłączone, nie należy go włączać.
2. Nie można wkładać lub wyjmować baterii – niektóre z urządzeń posiadają archaiczną strukturę i ingerowanie w ich architekturę może spowodować nieodwracalne uszkodzenia mechaniczne lub systemowe.
3. Należy unikać jakichkolwiek ingerencji i naciskania przycisków, jeżeli są dostępne.

4. Sfotografować i opisać w sposób jak najdokładniejszy znalezione urządzenie. Jeżeli posiada wyświetlacz, koniecznie należy uwzględnić jego wyświetlaną zawartość.
5. Przydatne informacje umożliwiające identyfikację znalezionego urządzenia i potencjalne jego przeznaczenie można sprawdzić w bazie znajdującej się pod adresem www.elibrary.usss.treas.gov[231].
6. Urządzenia tego typu powinny być poddawane jak najszybszej analizie z uwagi na duże ryzyko uszkodzenia.
7. Jeżeli wymagane jest przetransportowanie zabezpieczonego sprzętu, należy zachować szczególną ostrożność przy transportowaniu i zabezpieczyć sprzęt w odpowiednim pojemniku chroniącym przed uszkodzeniami mechanicznymi, czynnikami środowiskowymi i osobami postronnymi.
8. System wykorzystywany w tego typu urządzeniach jest często autorską wersją oprogramowania stworzonego przez hakera. Dane zmagazynowane na dysku mogą być zaszyfrowane.
9. Należy przeszukać okolicę w poszukiwaniu podobnych urządzeń.

Potencjalne dane, mogące stanowić dowody, jakie mogą zostać odnalezione:

1. Dane zawarte na dysku urządzenia – pliki audio/video, obrazy cyfrowe, pliki tekstowe.
2. System.
3. Połączenia z siecią internetową, teleinformatyczną.
4. Daty i godziny.
5. Historię połączeń.
6. Zasięg urządzenia.
7. Przeznaczenie urządzenia.
8. Dana adresata i odbiorcy nielegalnie uzyskanych danych.

Podanie wszystkich rodzajów urządzeń cyfrowych, jakie możliwe są do zabezpieczenia w celu odnalezienia śladów cyfrowych i uzyskaniu w efekcie materiału dowodowego, wykracza poza ramy tej pracy. Przedstawiono jedynie najpopularniejsze urządzenia z różnych grup urządzeń cyfrowych, począwszy od sprzętów prywatnych i domowych, biurowych, przenośnych, kończąc na typowych urządzeniach używanych w celach przestępczych. Przedstawienie szczegółowej analizy technik badawczych w zakresie pamięci cyfrowej wymaga posiadania specjalistycznej wiedzy z zakresu informatyki, dlatego też zostały opisane jedynie metody z kategorii możliwych do podjęcia w ramach czynności kryminalistycznych.

---

[231] https://www2.einformation.usss.gov/eInformation/home.seam?cid=559.

3. Zabezpieczanie śladów połączeń

Mianem połączenie cyfrowego nazywamy wszelką komunikację zachodzącą pomiędzy urządzeniami cyfrowymi w sieciach internetowych i teleinformatycznych. Najważniejszymi rodzajami połączeń, najczęściej wykorzystywanymi, a także dającymi najlepsze efekty o charakterze wykrywczym są połączenie telefoniczne. Sama idea połączenia cyfrowego skupia się na komunikacji i przesyłaniu pakietów danych pomiędzy jednym urządzeniem a drugim. Przykładowo, telefon komórkowy wysyłający żądanie połączenia z innym aparatem staje się nadawcą pakietu danych w momencie, gdy nadawca, czyli aparat telefoniczny będący docelowym urządzeniem, do którego wysłane są dane odpowie, staje się adresatem. W sieci teleinformatycznej u operatora zostaje odnotowane połączenie, naliczane są jego koszty, długość połączenia, miejsce, z którego dzwoniono, jakim aparatem telefonicznym się posłużono, kto jest właścicielem umowy zawartej na wykorzystaną usługę, miejsce pobytu adresata, długość połączenia. Dane takie są często wykorzystywane przez funkcjonariuszy organów ścigania w celu uzyskania śladów cyfrowych w danej sprawie. Samo połączenie pomiędzy urządzeniami i pozostawienie jego wykazu w bilingach operatora stanowi już ślad cyfrowy.

Z punktu widzenia praktycznego i potencjalnej przydatności badania kryminalistycznego śladów połączeń telefonicznych są one niezaprzeczalne najpowszechniejsze i zabezpieczanie ich przynosi często pozytywne efekty. W przypadku, gdy zwrócimy uwagę na inny typ połączenia – zachodzący pomiędzy komputerami, który działa na bardzo podobnych zasadach co połączenia telefoniczne, zauważymy, że mimo początkowego podobieństwa, opierającego się na przesyle pakietów danych, połączenie to może mieć nieporównywalnie bardziej skomplikowaną strukturę. W odróżnieniu od telefonów, gdzie dane są przesyłane od nadawcy, przez nadajnik operatora do adresata, sieć komputerowa może się składać z od kilku do kilkuset potencjalnych miejsc, gdzie wysłany pakiet danych zostanie przekierowany w stronę adresata. Szczególnie trudne do namierzenia i analizy kryminalistycznej są ślady nieautoryzowanego wejścia w obcy system z zagranicy. Liczba możliwych ścieżek i kombinacji, jakie trzeba sprawdzić podczas analizy, wymaga olbrzymich nakładów pracy i czasu. Dużo łatwiejsze w zabezpieczaniu i analizowaniu połączeń komputerowych są te, które obyły się na terenie tego samego kraju. Do najczęściej sprawdzanych połączeń należą te odnoszące się do przesyłania wiadomości pocztą elektroniczną, śledzenia, aktywności i wyszukiwania określonych słów przez użytkownika sieci internetowej (np. jak skonstruować bombę, zamach, grupy terrorystyczne, monitorowanie połączeń

z określonymi stronami, np. zawierającymi materiały o charakterze pedofilskim). Operatorzy i funkcjonariusze monitorują sieć w poszukiwaniu śladów cyfrowych wyżej wymienionych rodzajów połączeń komputerowych. Skuteczność wykrywania takiego rodzaju połączenia, które zostało nadane z terenu Rzeczpospolitej Polskiej, jest bardzo wysoka.

Trzecim rodzajem połączeń poza telefonicznymi i komputerowymi są te wykorzystywane przez inne urządzenia, np. sprzęty biurowe, przemysłowe, naukowe lub gospodarstwa domowego. Przykładowo, mogą być to sygnały inicjujące włączanie i wyłączanie się świateł drogowych, zraszaczy przeciwpożarowych w budynkach administracyjnych, sprzęty medyczne w szpitalach itp. Działalność przestępcza mająca na celu zakłócenie poprawnego przesyłania tego typu danych zdarza się rzadko i ma najczęściej charakter chuligański. Zdarzają się także przypadki wykorzystywania urządzeń zagłuszających wysyłanie sygnałów. Możliwe jest umieszczenie w urządzeniach komputera pokładowego samochodu osobowego urządzenia zakłócającego poprawne działanie systemów bezpieczeństwa i namierzania w celach późniejszego dokonania np. kradzieży danego pojazdu.

W celu zaistnienia połączenia w trzeciej grupie wzajemnego komunikowania się urządzeń cyfrowych może zostać wykorzystana każda istniejąca sieć przesyłowa. Począwszy od internetowej, przez teleinformatyczną i kończąc na połączeniach sieci rajdowej. Znaną i często zwalczaną formą wykorzystywania połączeń z omawianej grupy są kradzieże sygnału telewizyjnego lub radiowego. Osoby popełniające przestępstwo kradzieży sygnału popełniają czyn nazywany piractwem telewizyjnym, określony w art. 278 KK.

Kolejność czynności postępowania w sprawie przestępstwa komputerowego lub teleinformatycznego, polegająca na zabezpieczaniu połączenia cyfrowego, opiera się na kilku podstawowych zasadach. Głównym celem jest wykrycie sprawcy przestępstwa i postawienie go przed wymiarem sprawiedliwości dzięki dokładnemu i precyzyjnemu rozpoznaniu otoczenia, w jakim porusza się sprawca i identyfikacji technik cyfrowych, jakich używa w celu realizacji swoich planów. We wstępnej fazie prowadzonego postępowania najważniejsze jest zawężenie obszaru poszukiwań poprzez zlokalizowanie źródła sygnału lub połączenia cyfrowego, wykorzystując np. w tym celu adresy IP. Gdy obszar działań zostanie ustalony, należy zabezpieczyć w jego obrębie urządzenia mogące zawierać potencjalne dowody w sprawie i określić wstępną wersję przebiegu działania. Dokładne rozpoznanie przedmiotu przestępstwa komputerowego, jego otoczenia i właściwości jest istotnym czynnikiem powodzenia całego postępowania, którego głównym celem jest umożliwienie zebrania materiału dowodowego w najlepszy możliwy sposób, tzw. ograniczający ryzyko związane ze zniszczeniem, modyfikacją lub uszkodzeniem danych istotnych dla sprawy, a także eliminując przypadek, w którym zostaną pominięte działania, w wyniku których nie zostaną zebrane i zabez-

pieczone informacje istotne dla sprawy[232]. Przed przystąpieniem do zabezpieczania wybranego i sprecyzowanego już typu urządzenia należy ustalić, czy stanowi on jednolitą całość, czy jest częścią większej sieci lub jedynie urządzeniem pośrednim przekazującym sygnały cyfrowe w różnych kierunkach, np. nadajniki lub przekaźniki. Istotne są szczególnie właściwości danego urządzenia i otoczenie, w którym się znajduje – podjęcie złej decyzji wynikającej ze złego rozpoznania będzie rzutować w konsekwencji na efekt prowadzonego postępowania przygotowawczego. Gdy już uzyskane zostaną informacje na temat właściwości i struktury danych urządzeń, wymagane jest ustalenie sieci i systemów, w jakich przyjdzie operować. Możemy tutaj wyróżnić rodzaje systemów mobilnych, w jakie wyposażone są nowoczesne telefony komórkowe i tablety (Windows Mobile itp.) oraz systemy stacjonarne: Windows, Linux, Novell lub Unix. Zdarzają się przypadki, gdy na urządzeniu występują więcej niż jeden podstawowy system operacyjny. Brak odpowiedniej wiedzy z zakresu operowania w różnych systemach (systemy heterogeniczne) może wpłynąć bardzo negatywnie na wyniki analizy danych cyfrowych zawartych na nośnikach pamięci w takim urządzeniu. Zakres przeprowadzonego rozpoznania będzie rzutował również na materiał dowodowy, jaki zostanie pobrany od jednej maszyny, np. pojedynczego komputera lub wielu, gdy pracuje w sieci cyfrowej i dane zostały rozmieszczone na wielu urządzeniach. Osoby przygotowujące się do zabezpieczania urządzeń cyfrowych muszą również uzyskać odpowiedź na pytanie, czy zabezpieczane urządzenia stanowią dowody same w sobie, czy też są narzędziami popełnionego przestępstwa. Wszystkie te informacje i okoliczności będą wpływać zasadniczo na zaplanowanie kolejnych działań. W zależności od efektów przeprowadzonego rozpoznania w dalszej kolejności należy zaplanować rodzaje czynności, jakie trzeba będzie przeprowadzić, jaki będzie ich zakres oraz przebieg, w szczególności uwagę należy zwrócić na:

1. Przygotowanie odpowiednich narzędzi potrzebnych do analizy informatycznej, ale także takich, które będą niezbędne do demontażu części lub całości urządzenia.
2. Zebrać wszystkie odpowiednie dokumenty i druki niezbędne do poprawnego przeprowadzenia przeszukania i oględzin miejsca zdarzenia, wliczając w to także postanowienia sądu czy też prokuratora o przeprowadzeniu przeszukania.
3. Zapewnić odpowiednie warunki pracy dla biegłych i specjalistów z dziedzin wymaganych do poprawnego zabezpieczenia urządzeń i zapewnienie udziału w oględzinach osób posiadających wymaganą wiedzę informatyczną adekwatną do sytuacji.
4. Koniecznie trzeba zadbać o wystarczającą ilość pojemników służących do zabezpieczenia urządzeń cyfrowych przed czynnikami zewnętrzni i ingerencją

[232] A. Machnacz: *Współpraca organów ścigania w zakresie gromadzenia i zabezpieczania materiału dowodowego z przestępstwa w komputerach realizowanych za pośrednictwem sieci*, [w:] *Ius est ars boni et aequi,* red: P. Bogdalski, W. Pływaczewski, I. Nowicki, Szczytno 2008, s. 57.

osób nieupoważnionych. W tym miejscu należy zaznaczyć, że mianem „pojemnika" mogą być wszelkie środki transportu spełniające wyżej wymienione kryteria. Zapewnienie środka transportu w sytuacji, gdy wymagane będzie przetransportowanie zabezpieczonych urządzeń cyfrowych w pojemnikach do specjalistycznej analizy kryminalistyczno-informatycznej w laboratorium, o ile przepisy prawa na to zezwalają.

5. Przygotować wniosek o wzajemną pomoc prawną w dziedzinie środków tymczasowych w przypadku, kiedy konieczne jest do sprawy uzyskanie materiału dowodowego zlokalizowanego na terytorium innego państwa[233].
6. W pewnych sytuacjach zabezpieczenie obiektu siłami policyjnymi w celu niedopuszczenia osób nieuprawnionych.
7. W przypadku, gdy użytkownik informuje organ procesowy, iż na nośnikach informatycznych znajdują się dane stanowiące tajemnicę państwową, służbową czy dziennikarską, urządzenia zabezpiecza się technicznie zgodnie z przyjętymi w tym przypadku zasadami kryminalistycznymi (w odpowiednich pojemnikach), bez zapoznawania się z treścią. Zabezpieczone dane, urządzenia w opieczętowanych pojemnikach powinny być niezwłocznie dostarczone do właściwego sądu okręgowego, który to podejmie decyzję o ich ewentualnym odtajnieniu.

Należy również ustalić, czy na danym etapie postępowania wymagane będzie skontaktowanie się z odpowiednimi podmiotami w celu uzyskania dodatkowych informacji, środków, pomocy prawnej. Firmy zajmujące się dostarczaniem usług cyfrowych są źródłem wielu ważnych informacji. Działania użytkownika będącego klientem danej usługi zostają odnotowane – przykładem takich form kontroli są bilingi telefoniczne, zawierające dokładne dane na temat przeprowadzonych rozmów telefonicznych z określonego numeru. W przypadku, gdy mamy do czynienia z przestępstwem cyfrowym o podłożu międzynarodowym, należy ustalić, czy konieczne będzie skontaktowanie się z organami prawnymi innego państwa. Współpraca międzynarodowa na arenie cyfrowej odbywa się głównie dzięki istniejącym i podpisanym wzajemnym porozumieniom między danymi krajami, traktatom oraz umowom pomiędzy poszczególnymi państwami. Porozumienie i wzajemna pomoc organów z różnych krajów pozwala na podjęcie licznych i dużo bardziej skutecznych działań w celu zatrzymania sprawcy czynu zabronionego lub unieszkodliwienia danych znajdujących się na serwerach umieszczonych na terenie innego kraju.

W przypadku zabezpieczania śladów cyfrowych połączeń niezwykle ważne jest ustalenie źródła sygnału i pomieszczenia, w którym jest obecny sprzęt wymagany do zabezpieczenia. Odpowiednie odcięcie miejsca oględzin od osób postronnych stanowi fundamentalne znaczenie dla dobra zabezpieczanych śla-

---

[233] A. Machnacz: op. cit., s. 58.

dów cyfrowych. Każda ingerencja i nieupoważniony dostęp osoby trzeciej może spowodować nieodwracalne zatarcie lub zniszczenie potencjalnych dowodów w sprawie. Osoby prywatne mogą mieć istotny interes w uszkodzeniu materiału badawczego, np. prywatny komputer osobisty, by w ten sposób dokonać zatarcia śladów przestępstwa. Przedsięwzięcie takie pozwala na osiągnięcie szczególnych środków ostrożności.

Do pierwszych czynności na miejscu zdarzenia należy zabezpieczenie miejsca popełnienia przestępstwa przed zmianami, przez tzw. „zamrożenie sytuacji”[234], które polega na:

1. Fizycznym odcięciu osób od sprzętu komputerowego i wszystkich innych urządzeń cyfrowych mogących mieć bezpośredni wpływ na badane urządzenia lub będących z nimi połączone przez systemy teleinformatyczne.
2. Uniemożliwienie uzgodnienia zeznań świadków i wersji zdarzenia.
3. Niedopuszczenie do zniszczenia materiału dowodowego.

Często stosowaną techniką, gdy nie ma fizycznej możliwości na odcięcie zabezpieczanego obszaru w skuteczny sposób przed manipulacją cyfrową, zostaje odłączenie zasilania w sektorze (o ile nie zabrania tego obowiązujące prawo – wyłączenie zasilania na dużym obszarze może spowodować straty dla firmy i pracowników), w którym przeprowadzane są czynności zabezpieczania urządzeń cyfrowych. Postępowanie takie spowoduje oczywiście utratę danych ulokowanych w pamięci tymczasowej i ulotnej, może także spowodować uszkodzenia urządzeń i powstanie błędów cyfrowych. Odłączenie zasilania stanowi jednak dopuszczalną normę postępowania w przypadku, gdy inne możliwości zawodzą – wybór ten polega na zaakceptowaniu „mniejszego zła”, by skutecznie uniemożliwić wrogie działania cyfrowe. Warto też zaznaczyć, że odcięcie głównego źródła zasilania nie przyniesie oczekiwanego skutku, jeżeli w firmie lub budynku obecne są systemy awaryjnego zasilania.

W momencie, gdy obszar będzie już pod kontrolą funkcjonariuszy organów, należy zadbać o połączenia cyfrowe, odłączyć sieć teleinformatyczną przez zlokalizowanie serwerów i routerów wykorzystywanych w celu przesyłania danych.

4. Poszukiwanie i gromadzenie innego materiału cyfrowego

Poszukiwanie materiału dowodowego związanego z popełnionym przestępstwem komputerowych wiąże się z braniem pod uwagę wszelkich możliwych okoliczności związanych ze sferą cyfrową. Uzyskanie jak największej ilości

[234] A. Machnacz: op. cit., s. 59.

danych związanych ze zdarzeniem, rodzajem wykorzystanych technik informatycznych, użytym sprzętem cyfrowym i dodarcie do każdej przydatnej informacji powiązanej ze zdarzeniem. Głównym źródłem informacji na temat historii pracy z urządzeniami cyfrowymi i miejscem, w którym odnotowywane są wykonywane czynności, będą logi (rejestry) systemowe, obecne w większości urządzeń cyfrowych wyposażonych w systemy operacyjne. Logi mogą być gromadzone w bazie danych lub bezpośrednio w systemie. Dostęp do nich nie jest zabezpieczony i wymaga jedynie wiedzy z dziedziny informatyki. Istnieją różne rodzaje logów, niektóre występują w systemie, inne mogą być dostępne z poziomu określonych aplikacji. Warto zaznaczyć, że oddzielnymi logami mogą dysponować różne urządzenia cyfrowe. W praktyce podczas zabezpieczania sprzętów elektronicznych, np. komputerów, warto jest uzyskać logi z jak największej ilości źródeł. Urządzenia sieciowe mogą okazać się źródłem bardzo ważnych rejestrów, które nie zostały przykładowo odnotowanie w logach systemowych. Ograniczanie się do badania tylko jednego rodzaju typów danych cyfrowych lub zawężanie poszukiwania do ściśle określonego urządzenia, bez brania pod uwagę innych sprzętów powiązanych technicznie, nie jest wskazane.

Ważne jest również sprawdzenie baz danych policji, sprawdzenie informacji o osobach podejrzanych, a także o instytucjach powiązanych ze sprawą. Prześledzenie historii rozmów i kontaktów, uzyskanie dostępu do wykazów bilingów telefonicznych może okazać się istotnym źródłem informacji. Zawsze należy też zadbać o odpowiednie zebranie wyjaśnień od podejrzanych lub zeznań od świadków. Przydatne mogą okazać się także dzienniki pracy, np. administratorów systemu, w którym odnotowano działalność przestępczą. Firma prowadzi zawsze dokumentację dotyczącą monitorowania wewnętrznego sytemu. Znalezienie nieprawidłowości może mieć związek ze sprawą i dostarczyć kolejne cenne informacje. Wszystkie zbierane dane muszą jednak wykazywać się pełną wiarygodnością. Trzeba pamiętać, że pewne odnalezione dane mogą okazać się fałszywe lub być wynikiem celowego działania sprawcy, aby zmylić organy ścigania. Utalentowani hakerzy są w stanie bardzo skutecznie zacierać historię swojej działalności w cyberprzestrzeni.

Podczas zabezpieczania różnego rodzaju danych lub nośników cyfrowych zawierających dane trzeba mieć na uwadze współczesne zasady kryptograficzne. Ogólny dostęp w sieci internetowej do programów zapewniających kodowanie kryptograficzne jest w dzisiejszych czasach bardzo powszechny. Wielu użytkowników sieci wykorzystuje tego typu programy w celu chronienia danych newralgicznych lub takich danych, które mogą wywołać zainteresowanie określonych organów. W sytuacji natknięcia się przez funkcjonariuszy organów na tak zabezpieczone dane cyfrowe należy je pozostawić do wyłącznego opracowania przez eksperta z dziedziny informatyki. Próba otwarcia lub manipulacji tak zabezpieczonego pliku przez osobę nieprzygotowaną może uruchomić trudne i cza-

sochłonne do złamania algorytmy szyfrujące. W przypadku natknięcia się na dane zabezpieczone hasłem należy podjąć następujące działania:

1. Spróbować uzyskać od użytkownika informacje dotyczące sposobu przechowywania danych, organizacji pamięci masowej oraz wykonywania i przechowywania kopii zapasowych, a także identyfikatorów i haseł użytkowników oraz innych istotnych dla sprawy słów kluczowych.
2. Przeszukać wszystkie dostępne miejsca w celu zdobycia w/w informacji (w tym kosze na śmieci, meble znajdujące się w pomieszczeniu, notesy, odpady z niszczarki itp.). Każde skojarzenie słowa kluczowego z potencjalnym hasłem do komputera i systemu powinno zostać odnotowane[235].

Do podstawowych źródeł informacji możemy zaliczyć kilka elementów. Zadbanie o odpowiednie zagospodarowanie dostępnych środków może wpłynąć bardzo owocnie na przebieg postępowania. Najważniejszymi źródłami są:

1. Logi systemowe.
2. Dane cyfrowe przechowywane i zabezpieczone na nośnikach pamięci: dyskach twardych, w pamięci urządzeń przenośnych itp.
3. Kopie zapasowe i przechowywane tam dane.
4. Zeznania świadków.
5. Informacje uzyskane z dzienników i historii administrowania systemem.
6. Dokumentację powstałą w wyniku oględzin miejsca zdarzenia.
7. Rzeczy uzyskane w wyniku przeszukania pomieszczenia i osób.
8. Dodatkowe informacje z policyjnych baz danych dotyczące osób i instytucji.
9. Procedury dotyczące ochrony informacji w poszkodowanej instytucji.

Na koniec warto zwrócić uwagę na możliwość przesłuchania osoby pokrzywdzonej. Możliwe, że pokrzywdzony będzie mógł wskazać na cenne informacje dotyczące tego, co jego zdaniem mogło być przedmiotem przestępstwa, jakiego typu informacje mogły paść łupem sprawcy i kto mógł dokonać czynu zabronionego. Ze wszystkich zeznań należy sporządzić dokładną dokumentację.

5. Analiza zebranego dowodowego materiału cyfrowego

Podstawowym celem analizy zebranego materiału dowodowego związanego z przestępstwem komputerowym jest odpowiedź na pytanie dotyczące okoliczności zdarzenia i wykrycie sprawcy przestępstwa. W czasie analizy trzeba zwrócić uwagę na wszystkie zebrane materiały i informacje. Poprawne zinterpretowanie

[235] A. Machnacz: op. cit., s. 62.

wszystkich dostępnych środków może pokazać, co zostało skradzione lub naruszone, gdzie popełniono przestępstwo, kiedy działał sprawca, jakimi metodami się posłużono i jakich programów użyto, określenie celu sprawcy i dlaczego oraz kto popełnił czyn zabroniony[236].

W przypadku analizy logów zabezpieczonych w czasie postępowania wskazane jest utworzenie bazy powiązań dla każdego z połączeń, zwracając uwagę na następujące informację:

1. Data i czas rozpoczęcia oraz zakończenia połączenia.
2. Rodzaj połączenia (w sieci lokalnej, z/do sieci rozległej).
3. Wywoływane/wywołane adresy sieciowe.
4. Wykorzystane usługi i konta użytkowników.
5. Przesłane i odebrane bajty lub pakiety i ich długość.
6. Naruszenia – czyli zapisy określające wykonanie danego działania zakończone sukcesem lub porażką.
7. Różnice w stosunku do czasu lokalnego (określenie strefy czasowej), w tym wyróżnienie czasu systemowego oraz czasu rzeczywistego.
8. Inne informacje związane z przychodzącymi i wychodzącymi połączeniami.[237]

Dokładne przeanalizowanie logów może dostarczyć precyzyjnych informacji na temat niektórych kont użytkowników, stacji roboczych, adresów sieciowych i innych informacji będących powtarzalnymi sekwencjami lub śladem działalności użytkownika. W wyniku pełnej analizy zebranego materiału dowodowego wymagane jest sporządzenie szczegółowego raportu, uwzględniającego najistotniejsze informacje:

1. Wszelkie ustalone informację o zdarzeniu, razem z ich listą i dokładnym opisem.
2. Szczegółowo opisany sposób dokonanej analizy i na jakich danych były prowadzone badania.
3. Ustalony *modus operandi* sprawcy.
4. Przedstawienie metod, jakimi posłużył się sprawca, wliczając w to usługi sieciowe i urządzenia cyfrowe.
5. Opisanie rodzaju zastosowanego połączenia sieciowego.
6. Szczegółowy opis wszystkich podjętych działań w trakcie analizy i uzyskane rezultaty.
7. Jakie inne odrębne źródła informacji zostały wykorzystane w trakcie analizy, które umożliwiły sprawcy popełnienie przestępstwa.
8. Wyniki przeprowadzonej analizy.
9. Podsumowanie analizy.
10. Wnioski końcowe.

---

[236] Siedem złotych pytań kryminalistyki znajduje swoje zastosowanie także w przestępstwach na tle cyfrowym.

[237] A. Machnacz: op. cit., s. 64.

6. Znaczenie prawidłowego zabezpieczenia technicznego i procesowego śladów cyfrowych

W praktyce zabezpieczanie śladów cyfrowych powinno następować natychmiast po ich ujawnieniu, tworząc zabezpieczoną kopię wybranego fragmentu pamięci. Ślad cyfrowy pozostawiony bez ochrony jest niezwykle podatny na zniekształcenie lub zamazanie i aby mygł być wykorzystany w procesie i stać się materiałem dowodowym, musi być prawidłowo zabezpieczony. Podobnie jak w innych dziedzinach kryminalistyki, np. daktyloskopii, mechanoskopii itp., również przy śladach cyfrowych wyróżniamy następujące formy zabezpieczania śladów:

1. Zabezpieczanie procesowe.
2. Zabezpieczanie fotograficzne.
3. Utrwalanie techniczne śladu[238].

Zabezpieczanie procesowe śladów cyfrowych jest sprawą niezmiernie ważną we współczesnym świecie, nastawionym na cyfryzację społeczeństwa. Niewłaściwie zabezpieczony procesowo ślad może być ze względów formalnych odrzucony jako środek dowodowy. Zgodnie z art. 143 §1 KPK z przeprowadzonych oględzin obligatoryjnie sporządza się protokół. Zabezpieczanie procesowe nośników śladów cyfrowych polega zatem na ich szczegółowym opisie w protokole po analizie danych dostarczonych do badań informatyczno-kryminalistycznych. Natomiast sam ślad cyfrowy (*sensu stricto*) będzie ujawniany i badany przez biegłego podczas wykonywania ekspertyzy. W części opisowej opinii biegłego trzeba umieścić następujące dane o ujawnionym śladzie cyfrowym: miejsce znalezienia śladu (rejestry, logi, pliki itp.), metodę ujawnienia takiego śladu, czas, w jakim ślad cyfrowy powstał i z czym jest połączony (inne urządzenia, kontakty itp.). Dalsze informacje dotyczące śladu cyfrowego powinny zawierać: sposób zabezpieczenia – utrwalenie techniczno-informatyczne, czy ślad fotografowano (urządzenie, na którym się znajduje i ekran monitora), czy odnotowano jego obecność w innych dokumentach oględzinowych, cyfrowych lub materialnych, np. dzienniki administratora sieci.

Taki opis śladu cyfrowego w protokole oględzin z jednej strony spełnia funkcję zabezpieczenia dowodu, z drugiej zaś pozwala na kontrolę zabezpieczonego materiału dowodowego. Umożliwia to uzyskanie pewności przez organ ścigania,

---

238 Por. J. Kasprzak: *Kryminalistyka. Podręcznik dla Żandarmerii Wojskowej, cz I, Technika Kryminalistyczna,* Warszawa 1995, s. 54, E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka – czyli rzecz o metodach śledczych,* Warszawa 2008, s. 195.

sąd, a także przez oskarżonego i jego obrońcę, że dany konkretny ślad rzeczywiście został ujawniony na miejscu zdarzenia i jest pełnowartościowym dowodem w sprawie. Do zabezpieczenia procesowego można również zaliczyć metryczkę śladu, stanowiącą łącznik między zabezpieczeniem procesowym a utrwaleniem technicznym śladu.

Zabezpieczenie fotograficzne – powinno być dokonane zawsze, nawet wtedy, gdy ślad zabezpiecza się również innymi metodami. Niekiedy jest to sposób na zabezpieczenie informacji zawartych na ekranie urządzenia, gdy zostanie ono wyłączone w zły sposób i wszystkie informacje zostaną utracone. Zabezpieczenie fotograficzne poprzedza stosowanie innego rodzaju zabezpieczenia. Fotografowanie powinno się odbyć także zaraz po odnalezieniu istotnych danych i w taki sposób, by zapewnić czytelny i niepozostawiający żadnych wątpliwości obraz. Zdjęcia należy zrobić w pozycji naprzeciw ekranu, uwzględniając światło i kontrast obrazu. Fotograficzne zabezpieczanie śladów cyfrowych za pomocą aparatów fotograficznych to nie tylko fotografia samego ekranu, ale także całego urządzenia czy nawet ogólnoorientacyjna danego terenu lub pomieszczenia, gdzie miało miejsce badanie miejsca zdarzenia. Wskazuje się bowiem na charakter zdarzenia, na przedmioty, na których znajdują się ślady, w tym także ślady cyfrowe. Może to niekiedy pomóc w odtworzeniu pewnych zdarzeń i określeniu mechanizmów powstania śladu – co w przypadkach nietypowych może mieć bardzo duże znaczenie.

Utrwalenie techniczne śladu to takie jego zabezpieczenie, by mógł pozostać w niezmienionym stanie przez długi okres. W przypadku śladów cyfrowych utrwalenie techniczne następuje przy użyciu specjalistycznego oprogramowania i sprzętu komputerowego. Wybór odpowiedniego narzędzia przez eksperta z zakresu informatyki kryminalistycznej może zaowocować szybszym i efektywniejszym wynikiem.