https://doi.org/10.34836/pk.2022.316.2

Unikanie rejestrowania czynności użytkownika: TOR, Linux Tails

podkom. Sylwester Panasewicz[1]

[1] Laboratorium Kryminalistyczne Komendy Wojewódzkiej Policji w Białymstoku, sylwester.panasewicz@bk.policja.gov.pl

Streszczenie

Sieć TOR (The Onion Router) jest wirtualną siecią komputerową zapewniającą anonimizację oraz dostęp do często nielegalnych danych lub dla unikających cenzury. Linux Tails (The Amnesic Incognito Live System) stanowi natomiast system operacyjny bootowany wyłącznie z nośnika przenośnego (np.: pendrive, karty pamięci czy też płyty DVD) lub uruchamiany w sposób zwirtualizowany. Tails jako jedno z narzędzi oferuje dostęp do sieci TOR, zapewniając ponadto dalece wyszukane mechanizmy służące do unikania pozostawienia śladów cyfrowych na maszynie, z której korzysta użytkownik. Mimo innych intencji twórców obu omawianych powyżej narzędzi stały się one ulubionym pakietem olbrzymiej grupy przestępców na całym świecie. Autor w niniejszej publikacji skupia się na omówieniu zarówno obszarów powstawania śladów cyfrowych użytkowania TOR oraz Tails, jak i na możliwościach badawczych oraz możliwościach wnioskowania na ich podstawie. W pierwszej części artykułu opisany został mechanizm działania anonimizującej sieci TOR. Następnie autor zapoznaje czytelnika ze środowiskiem Linux Tails oraz odnosi się do faktycznych przypadków użycia.

Słowa kluczowe: anonimizacja, TOR, Tails, Linux, trasowanie, wirtualny

Jeszcze niedawno sen z oczu włamywacza spędzał problem, w jaki sposób pozostawić możliwie niewiele śladów na miejscu przestępstwa. Dziś, w dobie cyfrowej, sprawcy korzystają z różnorodnych narzędzi, by uzyskać nieuprawniony dostęp, fałszywą tożsamość lub dokonać innych działań, praktycznie nie pozostawiając śladów innych niż cyfrowe. Próbują ukryć się w cieniu zwykłego ruchu sieciowego, maskują swoją działalność, szyfrują dane stanowiące dowody cyfrowe. Niekiedy mogą wręcz powrócić na miejsce przestępstwa i kontynuować zacieranie śladów lub weryfikować ich istnienie bez wiedzy organów ścigania. Choć idea sieci anonimizujących czy elastycznych systemów operacyjnych typu live nie powstała z myślą o świecie przestępczym, jej owoce coraz częściej stają się takimi narzędziami. Skłoniło to autora do opisania w niniejszym artykule systemu operacyjnego Linux Tails, w charakterze narzędzia i zawartych w nim programów anonimizujących m.in. korzystających z sieci TOR, w kontekście kryminalistycznych badań informatycznych. Trzeba pamiętać jednak, że tego typu narzędzia są używane również m.in. przez ludzi żyjących w systemach autorytarnych lub osoby chcące zachować swoją prywatność. Czytelnicy, którzy mieli okazję zapoznać się z książką *Pamięć nieulotna* autorstwa Edwarda Snowdena, wiedzą, że podczas jego pracy dla NSA w kontakcie z prasą korzystał z systemu operacyjnego Tails. I co najważniejsze – nie został na tym przyłapany, co stanowi szczególną rekomendację.

Sieć TOR (The Onion Router) jest wirtualną siecią komputerową, w której zaimplementowano trasowanie cebulowe drugiej generacji, co zapobiega analizie ruchu sieciowego i zapewnia jej użytkownikom prawie anonimowy dostęp do zasobów Internetu.

Projekt TOR był początkowo sponsorowany przez laboratoria badawcze Marynarki Wojennej Stanów Zjednoczonych (U.S. Naval Research Laboratory) i rozwijany jako projekt militarny w celu ochrony komunikacji wywiadowczej USA w Internecie. Miał maskować działalność agentów wywiadu w sieci.

Inicjatorami sieci TOR byli programiści Roger Dingledine, Nick Mathewson oraz Paul Syverson, którzy przy wsparciu Centrum Badawczego Marynarki Wojennej USA rozpoczęli w 2002 r. pracę nad projektem. W 2004 roku na 13. Sympozjum Bezpieczeństwa Stowarzyszenia USENIX przedstawili pracę *Tor: The Second-Generation Onion Router*. W czasie od końca 2004 r. do listopada 2005 r. stał się on projektem

firmowanym przez Electronic Frontier Foundation (EFF). Obecnie rozwojem oprogramowania TOR zajmuje się Tor Project – niedochodowa organizacja non-profit o charakterze badawczo-edukacyjnym z siedzibą w Stanach Zjednoczonych, wspomagana przez wolontariuszy i użytkowników sieci na całym świecie. Projekt aktualnie funkcjonuje na licencji BSD, ale cały czas jest pośrednio sponsorowany przez Marynarkę Wojenną Stanów Zjednoczonych (Mider, 2019).

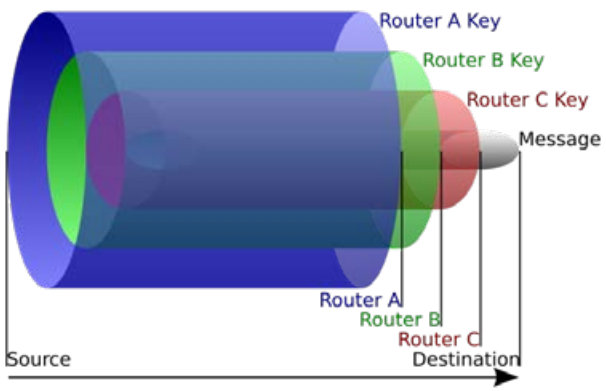
The Onion Router został udostępniony do użytku cywilnego w 2003 r. Serwery tworzące sieć TOR w początkowym okresie jej działania były umiejscowione jedynie w Stanach Zjednoczonych oraz Niemczech.

Nazwa sieci TOR jest skrótem od The Onion Router (router cebulowy). Pochodzi od techniki polegającej na wysyłaniu niezależnych i wielowarstwowo szyfrowanych pakietów, stąd określenie „trasowanie cebulowe". Tworzące tę sieć urządzenia realizują proces zwany trasowaniem cebulowym, odmiennym od klasycznego trasowania przez routery wykorzystujące model TCP/IP (Mider, 2019; Casad, 2017).

W sieci TOR dane są wysyłane zaszyfrowanymi warstwami, analogicznie do warstw cebuli. Zaszyfrowane w ten sposób dane są przesyłane przez serię węzłów sieciowych (routery cebulowe, ang. *onion routers*), z których każdy usuwa („odrywa") pojedynczą warstwę, odsłaniając kolejny cel przesyłanych danych. Gdy ostatnia warstwa zostanie odszyfrowana, dane docierają do miejsca docelowego. Nadawca pozostaje anonimowy, ponieważ każdy węzeł zna tylko lokalizację bezpośrednio poprzedzających i następujących węzłów. Router w każdej warstwie „wie" tylko to, co jest mu niezbędne do działania. Adresy IP wszystkich zapytań i odpowiedzi zmieniają się w każdym węźle (Ortega, 2022).

Trasowanie cebulowe jest strukturą danych utworzoną przez enkapsulowanie („zawijanie") danych w kolejne warstwy szyfrowania, które mogą być odszyfrowane przez tyle komputerów pośredniczących, ile jest warstw, zanim dotrą do miejsca docelowego. Połączenia pomiędzy każdym węzłem (serwerem proxy) jest szyfrowane. Pierwotne dane (i ich nadawca) pozostają ukryci, ponieważ dane są przesyłane pomiędzy węzłami pośrednimi, a żaden pośredni węzeł nie „zna" zarówno miejsca pochodzenia, jak i miejsca docelowego danych, dzięki czemu nadawca pozostaje anonimowy. Obserwacja takiego ruchu sieciowego nie pozwala stwierdzić, co jest w nim przesyłane.

Sieć TOR zapewnia anonimowość z wykorzystaniem protokołu TCP przy stosunkowo małym opóźnieniu i wysokiej przepustowości. Mechanizmy zaimplementowane w protokole sieci TOR nakładają warstwę anonimowości na warstwę TCP i tworzą ścieżkę (domyślnie minimum) trzypunktową, przez którą routery sieci TOR szyfrują warstwowo. Informacja o trasach jest przesyłana przez grupę autorytatywnych serwerów. W uproszczeniu: cała komunikacja TCP użytkownika jest tunelowana w jednym węźle, rotującym w czasie, a w celu zapewnienia niskich opóźnień sieć TOR nie wymusza retransmisji zgubionych pakietów.



Ryc. 1. Mechanizm trasowania cebulowego: źródło wysyła dane do routera A, który usuwa warstwę szyfrowania, aby dowiedzieć się tylko, gdzie wysłać je dalej i skąd pochodzą (chociaż nie „wie", czy nadawca jest źródłem, czy tylko innym węzłem). Router A wysyła je do routera B, który odszyfrowuje kolejną warstwę, aby poznać następne miejsce docelowe danych. Router B wysyła dane do routera C, który usuwa ostatnią warstwę szyfrowania i przesyła oryginalną wiadomość do miejsca przeznaczenia

Z perspektywy prywatności sieć TOR ma dwa cele:

1. Ukrywanie lokalizacji użytkowników korzystających z Internetu – wyśledzenie używanych przez nich adresów IP i lokalizacji ma być niemożliwe.
2. Szyfrowanie przesyłanych danych – sieć TOR szyfrując dane i przesyłając je routingiem cebulowym, ukrywa adresy IP użytkowników i przesyłane dane oraz ukrywa adresy IP operatorów ISP, poprzez których użytkownicy łączą się z siecią TOR (Ortega, 2022).

Węzły tworzące sieć TOR mają różne zadania i w zależności od charakterystyki i konfiguracji, rozróżniamy:

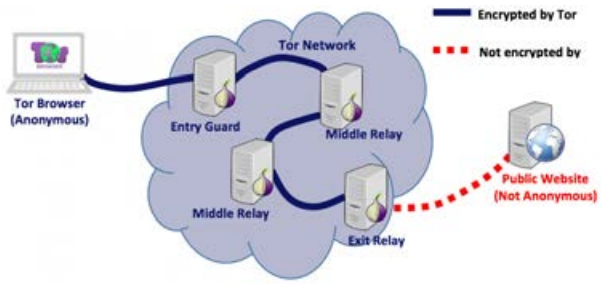
1. Węzły strażnicze (ang. *guard relays*) – komunikujące się z użytkownikami, połączone z resztą sieci TOR. Wykorzystywane od długiego czasu. Mają duże przepustowości.
2. Węzły przekaźnikowe (ang. *middle relays*) – komunikujące się wyłącznie z innymi węzłami. Dane, które z nich wychodzą, nie opuszczają sieci TOR.
3. Węzły wyjściowe (ang. *exit relays*) – punkty końcowe (brzegowe) sieci TOR. Odbierają żądania,

przesyłają je do odbiorców, odbierają odpowiedzi i wysyłają je w sieć w kierunku nadawcy.

4. Węzły pomostowe (ang. *bridge relays*) – będące węzłami, o których nie ma informacji w jawnym katalogu węzłów sieci TOR, które znacznie trudniej jest zablokować. Korzysta się z nich, gdy operator ISP blokuje sieć TOR. Lista ta jest dostępna na stronie https://bridges.torproject.org (Ortega, 2022).

Korzystanie z sieci TOR wygląda następująco:

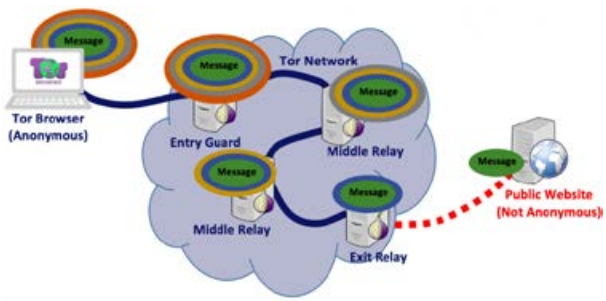
1. Host łączący się z siecią TOR pobiera listę dostępnych węzłów i wybiera trzy z nich: strażniczy, przekaźnikowy i wyjściowy.
2. Dane przeznaczone do wysłania przez sieć TOR są najpierw szyfrowane. Tylko węzeł wyjściowy zna adres żądanej usługi sieciowej i ma wgląd w przesyłane pakiety danych, ale ich pochodzenie nie jest mu znane, co zapewnia prywatność użytkownikowi.
3. Zaszyfrowane dane są ponownie szyfrowane i tylko węzeł przekaźnikowy wie, do którego węzła wyjściowego ma je przesłać. Dzięki podwójnemu szyfrowaniu tylko węzeł strażniczy wie, gdzie znajduje się węzeł przekaźnikowy (Ortega, 2022).



Ryc. 2. Diagram pokazujący typowy scenariusz działania klienta sieci TOR uzyskującego dostęp do publicznej strony w sieci Internet

Dane są szyfrowane, zanim opuszczą komputer użytkownika:

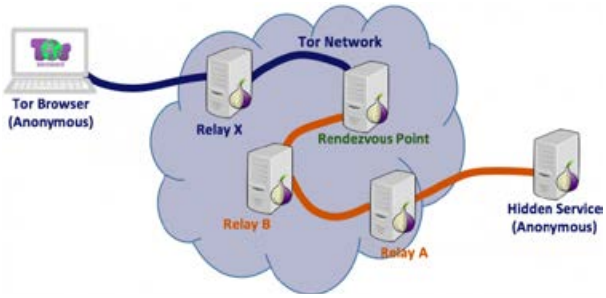
1. Jeśli istnieje system monitorujący połączenie internetowe (może to zrobić ISP), widzi on tylko zaszyfrowane dane wymieniane z węzłem strażniczym.
2. Tylko węzeł strażniczy widzi IP użytkownika i wie, gdzie znajduje się węzeł przekaźnikowy.
3. Tylko węzeł przekaźnikowy wie, gdzie są węzły strażniczy i wyjściowy. Nie wie jednak, gdzie jest użytkownik ani żądana strona internetowa (lub inna usługa sieciowa). Węzły przekaźnikowe nie znają swoich miejsc w sieci.
4. Węzeł wyjściowy wie, gdzie jest żądana strona internetowa (lub inna usługa sieciowa) i węzeł przekaźnikowy. Ale nie wie, gdzie jest użytkownik i węzeł strażniczy (Ortega, 2022).



Ryc. 3. Diagram pokazujący jak wiadomość będzie podróżować poprzez sieć TOR dopóki nie dotrze do publicznej witryny internetowej. Klient sieci TOR (przeglądarka Tor Browser) dodaje tyle warstw, ile jest przekaźników w łańcuchu

Niektóre sieci blokują ruch wychodzący na porcie TCP 9050 używanym przez sieć TOR, a nawet dynamicznie wciągają na czarną listę wszystkie węzły sieci TOR, uniemożliwiając korzystanie z tej sieci. Ograniczenie to można ominąć, używając tzw. mostków sieciowych, czyli węzłów sieci TOR niewidocznych w publicznym katalogu sieci (Allsopp, 2017).

Oprócz łączenia się z usługami w Internecie sieć TOR umożliwia korzystanie z tzw. ukrytych usług (*hidden services*), świadczonych na całkowicie anonimowych serwerach sieciowych zamkniętych w ekosystemie sieci TOR i widocznych tylko w niej, które korzystają z własnego rozproszonego systemu adresowania (Allsopp, 2017).



Ryc. 4. Diagram przedstawiający mechanizm uzyskiwania dostępu do serwera WWW ukrytego w sieci TOR (ukrytej usługi): (1) jeden serwer Tor Relay (przekaźnik) zostanie wybrany jako (przekaźnik) Rendezvous Point; (2) tworzone są dwa połączenia: jeden od klienta sieci Tor do węzła Rendezvous Point, a drugi od ukrytego serwera w sieci Tor do węzła Rendezvous Point. Autor uważnemu czytelnikowi pozostawia pod rozwagę, czy Hidden Service na powyższym diagramie nie powinien być objęty obszarem obrazowej chmury Tor Network

W przeciwieństwie do zwykłych stron internetowych, do których uzyskuje się dostęp za pomocą ich adresów URL, dostęp do ukrytych usług uzyskuje się za pomocą specjalnego typu adresów *onion*, zawierających losowy, niemnemoniczny ciąg znaków i niebędących

 https://doi.org/10.34836/pk.2022.316.3

Badania autentyczności numerów identyfikacyjnych

Ewa Jędrych[1], nadkom. Robert Mróz[1], kom. Krzysztof Biskup[1]

[1] Centralne Laboratorium Kryminalistyczne Policji, robert.mroz@policja.gov.pl, krzysztof.biskup@policja.gov.pl

Streszczenie

Niniejszy artykuł przedstawia podstawowe definicje takich pojęć jak numer VIN i tabliczka znamionowa. Opisane zostały również metody identyfikacji pojazdów oraz metody ujawniania ingerencji pozafabrycznej w oznaczenia identyfikacyjne. Na przykładach przedstawiono również sposoby przerabiania oznaczeń identyfikacyjnych i wymiany fragmentu karoserii z numerem VIN na inny fragment karoserii z innym numerem VIN celem zalegalizowania pojazdów pochodzących z czynów zabronionych.

Słowa klucze: oznaczenie identyfikacyjne, numer VIN, ujawnianie znaków, samochód, tabliczka znamionowa, pole numerowe, podzespoły samochodowe, kryminalistyka

W zwalczaniu przestępczości samochodowej jednym z kluczowych elementów jest ustalenie oryginalnego numeru identyfikacyjnego pojazdu – VIN (Vehicle Identification Number). Numer identyfikacyjny pojazdu jest nadawany przez producenta i umieszczany w określonych miejscach pojazdu. Przed 1981 r. nie było przyjętego jednego standardu określającego ten numer i producenci stosowali do jego oznaczenia różne formaty. Współczesny numer VIN składa się z 17 znaków – cyfr i liter, z wyłączeniem liter I, O oraz Q. W Unii Europejskiej numer VIN nadawany jest według normy ISO-3779, w Ameryce Północnej natomiast format zawiera dodatkową cyfrę kontrolną, ale jest kompatybilny z europejskim. W polskim prawodawstwie numery identyfikacyjne pojazdów zawarto w ustawie Prawo o ruchu drogowym. Poprzez numery identyfikacyjne należy rozumieć wymienione w ww. ustawie cechy identyfikacyjne, a zatem numer nadwozia VIN, numer podwozia, a także numer ramy. Do niedawna cechą identyfikacyjną był również numer silnika, jednak 21 października 2005 r. weszła w życie ustawa z dnia 29 lipca 2005 r. o zmianie ustawy o transporcie drogowym oraz niektórych innych ustaw (Dz. U. Nr 180 poz. 1497), która zmieniła między innymi wymagania ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym, uchylając przepisy dotyczące numeru silnika jako cechy identyfikującej pojazd.

Funkcjonariusze Policji prowadzący postępowanie w sprawie związanej z przestępczością samochodową szukają przede wszystkich odpowiedzi na pytania:

1. Czy w samochodzie występuje oryginalny numer VIN?
2. Jeśli numer VIN jest oryginalny, to czy identyfikuje on pojazd? Zdarza się bowiem, że przestępcy wstawiają wprawdzie oryginalny numer VIN, lecz taki, który został wycięty wraz z podłożem z innego pojazdu, np. zniszczonego w wyniku wypadku.
3. Czy oznaczenia występujące na podzespołach samochodowych mogą służyć do identyfikacji indywidualnej podzespołu, a przez to do uzyskania numeru VIN pojazdu, w którym podzespół został fabrycznie zamontowany?

Każdy pojazd składa się z tysięcy podzespołów, a tylko niektóre z nich służą do identyfikacji pośredniej pojazdu. Numer VIN jest oznaczeniem trwale naniesionym na elemencie konstrukcyjnym pojazdów. Element konstrukcyjny, na którym znajduje się przedmiotowe oznaczenie, musi być trwale połączony z pozostałą częścią karoserii. Dostęp do miejsca, w którym znajduje się oznaczenie identyfikacyjne, powinien być łatwy i niewymagający demontażu elementów wyposażenia pojazdu. Producenci nanoszą oznaczenie VIN na karoserię lub ramę w różnych miejscach, w zależności od marki i modelu pojazdu. Numer VIN może znajdować się w przedziale silnikowym (w przedniej części pojazdu), przedziale pasażerskim lub w przedziale bagażowym. Miejsce naniesienia oznaczenia VIN opisane jest w karcie homologacji – dokumentacji dopuszczenia pojazdu do obrotu na dany rynek, np. Unii Europejskiej. VIN jest siedemnastoznakową

kombinacją nadawaną przez wytwórcę, która umożliwia określenie fabryki, marki, typu pojazdu, indywidualnego numeru produkcyjnego. Ponadto niektórzy producenci kodują w tym numerze rok produkcji pojazdu oraz fabrykę, w której tenże pojazd został wyprodukowany. Ogólnie rzecz biorąc, cały kod (nr VIN) podzielony jest na trzy sekcje:

a) **CZĘŚĆ WMI.** WMI, czyli World Manufacturers Identification, oznacza tzw. światowy znak producenta, który tworzą trzy znaki numeru VIN. Kody WMI przyznawane są przez Narodową Organizację (w Polsce przez Przemysłowy Instytut Motoryzacji), a rejestrowane i sprawdzane przez działającą z upoważnienia ISO organizację, np.: S.A.E. Society of Automotive Engineers, Inc. Pierwszy znak WMI to zakodowane oznaczenie kraju, w którym wyprodukowano pojazd, np. w pojazdach wytwarzanych w USA na pierwszym miejscu w znaku znajduje się cyfra „1" albo „4", w Kanadzie cyfra „2", w Japonii literę „J", a we Francji literę „V". Drugi znak WMI określa konkretnego producenta (firmę, koncern) pojazdów, np. Audi (A), BMW (B), Ford (F), General Motors (G), Honda (H), Mercedes Benz (D), Nissan (N), Toyota (T), Volvo (V). Trzeci znak WMI oznacza typ produkowanego pojazdu, np. dla Volkswagena oznaczenie „WVW" stosuje się w samochodach osobowych (ryc. 2.), zaś „WV2" jest właściwe dla samochodów dostawczych. Jeśli jednak dana firma produkuje mniej niż 500 pojazdów rocznie, trzeci znak numeru VIN stanowi zawsze cyfra „9".

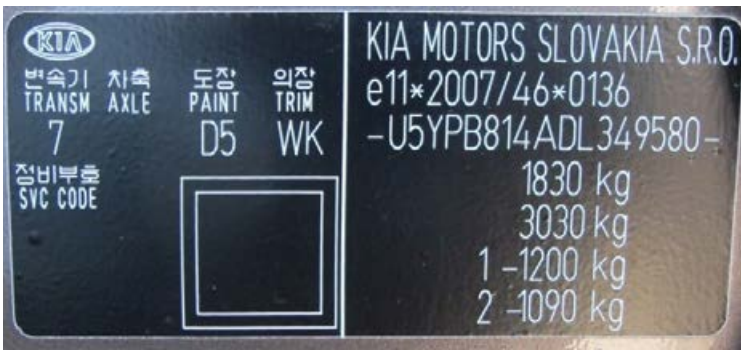
b) **CZĘŚĆ VDS.** VDS, czyli Vehicle Description Section, to druga część numeru identyfikacyjnego pojazdu, która składa się z sześciu znaków i jest przeznaczona do jego opisu. Znaki oraz ich kolejność i znaczenie określane są przez producenta i powinny charakteryzować konstrukcję pojazdu, rodzaj nadwozia, typ silnika bądź inne istotne cechy. W tej dziedzinie panuje absolutna dowolność. Nawet ten sam producent w zależności od modelu, roku produkcji czy kraju odbiorcy stosuje często inne oznakowanie pojazdu. Stosunkowo jasne kryteria oraz konsekwentne znakowanie realizuje np. firma Mercedes czy BMW.

c) **CZĘŚĆ VIS.** VIS, czyli Vehicle Identification Number, to tzw. sekcja identyfikująca pojazd, składająca się z ośmiu znaków, przy czym cztery ostatnie muszą być cyframi. Pierwszy znak określa rok produkcji pojazdu, który jest zakodowany za pomocą cyfr od „0" do „9" oraz liter z alfabetu łacińskiego z wyłączeniem liter takich jak „I", „O", „Q", „U". Drugi symbol to oznaczenie fabryki bądź montowni, w której pojazd został zbudowany. Jednakże od ww. oznaczeń są odstępstwa, gdyż niektórzy producenci nie umieszczają roku modelowego pojazdu oraz montowni w numerze VIN. Pozostałe miejsca są do dyspozycji producenta, oczywiście o ile wytwarza on co najmniej 500 egzemplarzy rocznie, gdyż w przeciwnym razie musi on na trzecim, czwartym i piątym miejscu umieścić dodatkowy indywidualny kod producenta. Najczęściej jednak te ostatnie sześć znaków VIN stanowią kolejny numer produkcyjny pojazdu, który jest przypisany pojedynczemu egzemplarzowi.

Ryc. 1. Przykład oznaczenia identyfikacyjnego VIN pojazdu marki Mercedes

Dodatkowym oznaczeniem identyfikacyjnym jest tabliczka znamionowa. Obowiązujące w Polsce przepisy prawa wymagają, aby każdy pojazd był w odpowiedni sposób oznaczony. Identyfikatorem każdego samochodu lub maszyny jest poza numerem VIN także tabliczka znamionowa, która zawiera podstawowe dane techniczne. Brak tabliczki uniemożliwi uzyskanie pozytywnego wyniku obowiązkowych badań technicznych.

Tabliczki znamionowe wykonywane są w różnych kształtach (prostokątne lub kwadratowe) i mogą



Ryc. 2, 3. Przykłady tabliczek znamionowych wykonanych w formie metalowej blachy oraz naklejki

przyjąć formę naklejki, płytki metalowej, płytki wykonanej z tworzywa sztucznego. Producenci pojazdów zabezpieczają tabliczkę znamionową przed wpływem warunków środowiskowych oraz przed próbą wtórnego montażu. Stosowane są różnego rodzaju zabezpieczenia, między innymi: naklejki zawierające w swojej budowie pigmenty emitujące np. logo producenta widoczne w świetle ultrafioletowym, wielowarstwowe folie, nacięcia uniemożliwiające odklejenie i hologramy. Tabliczki wykonane z metali lub tworzyw mogą być przyklejane lub mocowane za pomocą nitów lub jednorazowych kołków montażowych. Oznaczenia występujące na tabliczkach znamionowych wykonywane są różnymi metodami: grawerowania laserowego, druku laserowego, sitodruku, numeratorami stałymi lub znakowarkami punktowymi.

Badania pojazdów możemy podzielić na dwie grupy: badania nieniszczące i niewpływające na powłokę lakierniczą oraz badania niszczące, wpływające zarówno na powłokę lakierniczą, jak i na strukturę metalu.

Badania nieniszczące są badaniami oceniająco-typującymi. W trakcie wykonywanych czynności używa się między innymi urządzeń powiększających, światła ultrafioletowego, defektoskopu stałomagnetycznego, mierników powłok lakierniczych. Podczas prowadzenia tych badań biegły wzrokowo oraz używając ww. urządzeń, ocenia wygląd, technologię wykonania oznaczenia oraz jakość naniesionych na polu numerowym powłok lakierniczych.

W badaniach niszczących – wpływających na strukturę powłoki lakierniczej oraz strukturę metali – wykorzystuje się zmywacze do usuwania powłok lakierniczych oraz odczynniki chemiczne do ujawniania zniszczonych oznaczeń. Usunięta powłoka lakiernicza odsłania strukturę metalu. W przypadku stwierdzenia niejednorodnej struktury, przebarwień, ciągłości metalu i deformacji znaków VIN przystępuje się do badań rekrystalizacyjnych, mających na celu ujawnienie usuniętych znaków i metody ingerencji w polu numerowym.

W czasie wykonywania badań biegły oceniający oznaczenia identyfikacyjne przeprowadza również ocenę połączenia elementu karoserii, na którym znajduje się numer VIN i tabliczka znamionowa, z pozostałą częścią karoserii lub ramy. Badania mają na celu określenie, czy element z numerem VIN stanowi integralną całość, a połączenia zgrzewane, nitowane lub sklejane wykonane zostały w czasie trwania procesu produkcyjnego lub napraw blacharsko-lakierniczych.

Metody ujawniania sfałszowanych oznaczeń identyfikacyjnych na metalowych podłożach

Ujawnianie usuniętych i nieczytelnych oznaczeń firmowych z pojazdów i innych metalowych wyrobów ma miejsce zwykle wtedy, gdy zachodzi potrzeba ustalenia pochodzenia samochodu lub przedmiotu bądź faktu usiłowania zmiany oznaczenia oryginalnego na wyrobach, co do których zachodzi podejrzenie, że pochodzą one z kradzieży. Najczęściej fałszuje się numery

Ryc. 4, 5. Badanie pola numerowego pojazdu z wykorzystaniem defektoskopu stałomagnetycznego

Ryc. 6. Badania niszczące z wykorzystaniem zjawiska rekrystalizacji

Ryc. 7. Badania niszczące – usunięcie powłoki lakierniczej w celu oceny połączeń elementu z numerem VIN z pozostałą częścią nadwozia

znajdujące się na samochodach, broni, urządzeniach pomiarowych oraz różnego rodzaju narzędziach. Przestępcy, aby utrudnić identyfikację skradzionego samochodu lub przedmiotu, starają się usunąć wszelkie znaki charakteryzujące taki samochód lub przedmiot, a przy tym zwykle na polu numerowym nanoszą nowe oznaczenia numerowe. Jedną z najczęściej stosowanych metod usuwania numerów identyfikacyjnych VIN z pojazdów jest zdejmowanie z powierzchni pola numerowego warstwy metalu do takiej głębokości, aż numer stanie się niewidoczny. Drugim etapem po całkowitym usunięciu lub zakryciu oryginalnych oznaczeń i przygotowaniu pola numerowego jest naniesienie nowego numeru o odmiennej treści. Czynności pozwalające na usunięcie oznaczeń identyfikacyjnych można wykonać metodami mechanicznymi, np. poprzez zeszlifowanie, wycięcie, zaklepanie, sfrezowanie, lub metodami termicznymi (rozgrzanie, napawanie). Usunąć oznaczenia można także przez wymianę całych elementów z oznaczeniami identyfikacyjnymi lub poprzez ich zakrycie innym materiałem. Po takim zabiegu pole pozostaje bez oznaczeń i najczęściej na to miejsce nanoszone są nowe znaki. Taki sposób usuwania znaków nie powoduje większych zmian w strukturze podłoża. Do najczęstszych metod usuwania, fałszowania oznaczeń identyfikacyjnych zalicza się:

- przerobienie niektórych cyfr lub liter na inne z zachowaniem fragmentów graficznych pierwotnego zapisu np. „3" na „8". Do najczęściej spotykanych metod przerabiania/fałszowania oznaczeń identyfikacyjnych w pojazdach samochodowych zalicza się: zmianę treści pojedynczych cyfr lub liter, przebicie pojedynczych znaków lub członów, zakrycie części oryginalnego oznaczenia, zmianę kolejności znaków tworzących numer identyfikacyjny lub dodanie cyfr lub liter na początku lub na końcu numeru;
- wycięcie całego pola numerowego lub jego fragmentu i uzupełnienie ubytku poprzez wspawanie w to miejsce innego fragmentu z numerem wyciętym z samochodu tej samej marki i modelu. Wycięte, a następnie wspawane fragmenty pochodzą najczęściej z pojazdów rozbitych lub spalonych, które nie nadają się już do naprawy;
- zaklepanie znaków przy użyciu młotka, punktaka lub przecinaka. Powoduje to znaczne deformacje w strukturze podłoża, co często uniemożliwia ujawnienie oznaczenia numerowego;
- usunięcie treści oznaczeń numerowych metodą termiczną, polegającą na nagrzaniu metalu palnikiem lub za pomocą elektrody do takiego stanu, w którym nastąpią zmiany w jego strukturze. Zmiany termiczne spowodują tzw. rozmycie wybitych znaków. Metal w procesie spawania ulega stopieniu, co powoduje zupełną przebudowę sieci krystalicznej. Naspawany metal stapia się z metalem podłoża tak, że nie jest możliwe odwarstwienie czy też oddzielenie spoiny od podłoża;
- zeszlifowanie całej treści oryginalnych oznaczeń i wyklepanie na gorąco pola, a następnie naniesienie nowego numeru za pomocą dobranych znaczników numerycznych zbliżonych kształtem i wielkością.

W procesie ujawniania znaków usuniętych z przedmiotów metalowych wykorzystuje się różnice struktury miejsc, gdzie naniesione były poszczególne znaki, w stosunku do pozostałej części powierzchni pola numerowego. Ujawnienie usuniętych oznaczeń numerowych jest możliwe wówczas, gdy zostały one naniesione w taki sposób, że nastąpiło naruszenie struktury metalu.

Do ujawnienia usuniętych znaków na wyrobach posiadających własności ferromagnetyczne (żelazo, nikiel, kobalt i ich stopy) wykorzystywana jest metoda magnetyczna (nieniszcząca). Metale ferromagnetyczne mają zdolność magnesowania się pod wpływem pola magnetycznego, przy czym miejsca odkształceń plastycznych (miejsca usunięcia oznaczeń numerowych) wskutek rozpuszczenia linii

Ryc. 8. Oznaczenie szkieletu pistoletu Buss odtworzone przy pomocy defektoskopu

Ryc. 9. Numer ujawniono za pomocą defektoskopu

Ryc. 10. Oznaczenie zamka karabinu Mosin odtworzone odczynnikiem chemicznym

Ryc. 11. Oznaczenie magazynka karabinu Mosin odtworzone odczynnikiem chemicznym

Ryc. 12. Narzędzia chirurgiczne wykonane ze stali nierdzewnej

Ryc. 13. Oznaczenie numerów narzędzi chirurgicznych odtworzone odczynnikiem chemicznym

sił pola magnetycznego wykazują zdolność przyciągania cząstek żelaznego proszku. Ujawniony obraz usuniętego oznaczenia identyfikacyjnego przedmiotu nie jest trwały, więc należy utrwalić go za pomocą aparatu fotograficznego.

Do ujawnienia usuniętych znaków najczęściej stosuje się metodę chemiczną (niszczącą) – polega ona na działaniu na powierzchnię metalu odpowiednimi odczynnikami chemicznymi. Miejsca, na których znajdował się znak (występują tu ziarna zgniecione, rozdrobnione lub innej wielkości niż w pozostałej części podłoża), ulegają szybszemu rozpuszczeniu. Po zakończeniu badań powierzchnia pola numerowego z ujawnionym oznaczeniem powinna być zabezpieczona i oczyszczona ze środków chemicznych, a także poddana ochronie antykorozyjnej.

W artykule przedstawiono między innymi oznaczenia stosowane przez producentów pojazdów celem ich identyfikacji. Dzięki identyfikacji można rozróżniać pojazdy oraz przypisać je do danego właściciela. Ponadto w opracowaniu ukazano sposoby fałszowania, przerabiania oznaczeń identyfikacyjnych oraz sposoby oceny ich oryginalności i ewentualnego ujawnienia metody przerobienia/podrobienia oznaczenia. Znajomość powyższych zagadnień pozwoli na zastosowanie tej wiedzy np. podczas oględzin czy zakupu pojazdu.