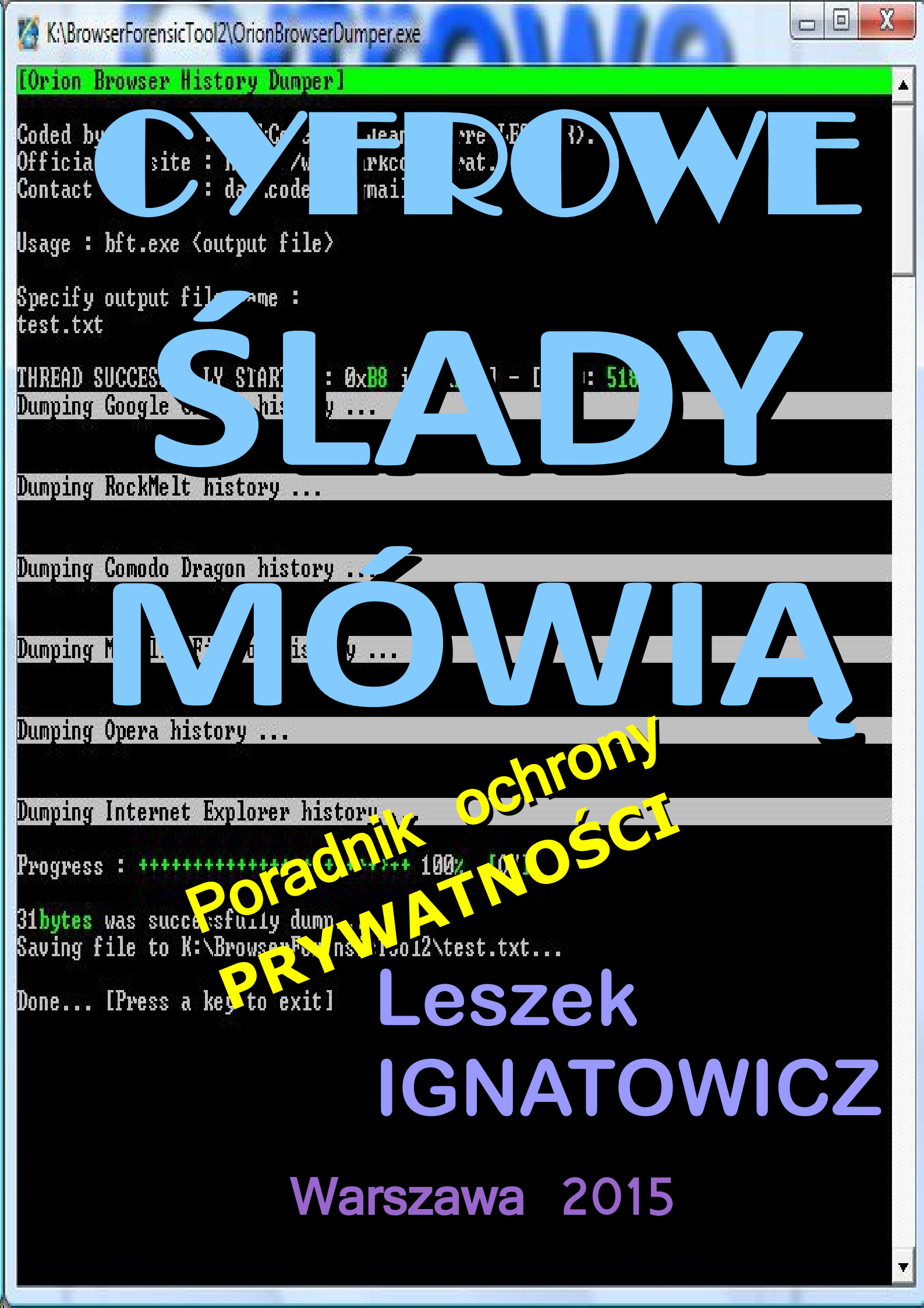

K:\BrowserForensicTool2\OrionBrowserDumper.exe
[Orion Browser History Dumper]
Usage : bft.exe <output file>
Specify output file name :
test.txt
Dumping Google Chrome history ...
Dumping RockMelt history ...
Dumping Comodo Dragon history ...
Dumping Opera history ...
Dumping Internet Explorer history ...
Progress : 100%
31bytes was successfully dumped
Saving file to K:\BrowserForensicTool2\test.txt...
Done... [Press a key to exit]
CYFROWE
ŚLADY
MÓWIĄ
Poradnik ochrony PRYWATNOŚCI
Leszek
IGNATOWICZ
Warszawa 2015

Na szukanie lepszego świata
nie jest jeszcze za późno.
Alfred Tennyson

Leszek IGNATOWICZ

Cyfrowe ślady mówią

Poradnik ochrony prywatności

ISBN 978-83-7853-406-8

Wydanie I, Warszawa 2015

Projekt okładki: Leszek IGNATOWICZ

Grafika na okładce: zrzut ekranu aplikacji *Orion Browser History Dumper*

Coded by DarkCoderSc (Jean-Pierre LESUEUR)

Korekta: Agnieszka Kwiatkowska

Kontakt z autorem: leszek@ignatowicz.net

Spis Treści

Wstęp – po co nam prywatność?

W październiku ubiegłego roku opublikowałem bezpłatnego ebooka *„Cyfrowe ślady. Jest się czego bać”*[1], który w przystępny sposób wyjaśnia zagrożenia naszej prywatności w cyfrowym świecie. Niestety, świadomość tych zagrożeń jest niewielka. Po części wynika to z propagowania poglądu, że jeśli nie masz nic do ukrycia, nie musisz niczego się obawiać, ujawniając, z własnej woli lub nieświadomie, prywatne informacje o sobie. Jest to jeden z argumentów podnoszonych przez amerykańską Agencję Bezpieczeństwa Krajowego (ang. National Security Agency, NSA), czy też globalne cyberkorporacje z Google i Facebookiem na czele. Jednak ujawniona przez Edwarda Snowdena[2] skala masowej inwigilacji z wykorzystaniem globalnej sieci Internet budzi niepokój. Więcej informacji na ten temat znajdziesz na anglojęzycznej stronie *https://nsa.gov1.info/*. *Śledzenie użytkowników Internetu* w celach komercyjnych też nie jest tak niewinne, jak wmawiają nam cyberkorporacje. Być może nie gromadzą one danych osobowych użytkowników swoich serwisów, lecz profilują ich pod kątem personalizacji usług, a zwłaszcza reklamy ukierunkowanej.

Nie ma jednej uniwersalnej odpowiedzi na postawione powyżej pytanie. Jeśli komuś wygodnie nie przejmować się utratą prywatności, jaką nieuchronnie powoduje korzystanie z Internetu, to jego prawo. Tego ebooka napisałem dla tych, którzy korzystając z obfitości zasobów Internetu, chcą też chronić swoją prywatność. Nie jest to takie trudne, nie wymaga zbyt wielu zabiegów, a pomoże uniknąć kłopotów.

---

[1] Leszek IGNATOWICZ, **„Cyfrowe ślady. Jest się czego bać”**, Warszawa 2014

Do bezpłatnego pobrania *http://pdf.helion.pl/s_5602/s_5602.pdf* lub is.gd/ifenek

[2] Glenn Greenwald, **„Snowden. Nigdzie się nie ukryjesz”**, Warszawa 2014

Metadane – ukryte informacje

Termin metadane (ang. metadata) oznacza „dane o danych”. Są one dołączane do plików zawierających różne dokumenty, fotografie, filmy, czy nagrania audio. Generalnie służą do celów zarządzania tymi plikami, co oznacza szybką identyfikację ich zawartości, wyszukiwanie itp. Nie są one jednak częścią dokumentu i w samym dokumencie są niewidoczne. Ich istnienie łatwo przeoczyć, a mogą zawierać istotne dane, których nie chcemy ujawniać. Metadane mogą więc zagrażać naszej prywatności.

Metadane w plikach Microsoft Office

Najwięcej metadanych zwierają powszechnie używane pliki tworzone przez edytor Microsoft Word – pliki binarne DOC, a w nowszych wersjach Worda pliki XML/zip, oznaczane rozszerzeniem DOCX. W metadanych tych plików można znaleźć nie tylko informacje dotyczące twórcy dokumentu, lecz także ostatnich 10-ciu użytkowników, edytujących ten dokument. Czasami zawierają również dziennik zmian w dokumencie.

Metadane są niewidoczne, lecz można użyć programu, który potrafi je odczytać, a nawet usunąć. Nowsze wersje pakietu MS Office (począwszy od wersji 2007) zawierają wbudowane narzędzie pozwalające na usunięcie metadanych. Natomiast metadane z plików w starszym formacie DOC można usunąć przy pomocy dalej omówionego programu Doc Scrubber.

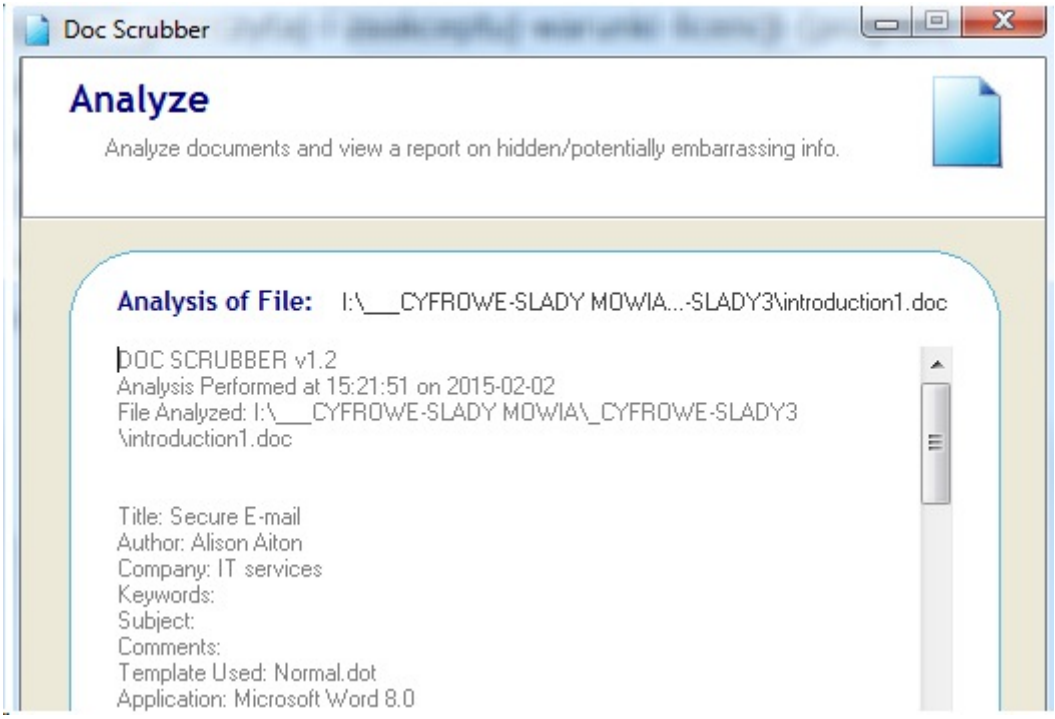
Pewnym ominięciem problemu metadanych w plikach Microsoft Office, jest zapisanie dokumentu w formacie PDF (od ang. portable document format). Ten format również zawiera pewne metadane, lecz można łatwo je edytować lub po prostu usunąć, o czym będzie mowa dalej.

Analiza i usuwanie metadanych z plików Word DOC

Bezpłatny, prosty w obsłudze program Doc Scrubber realizuje dwie funkcje: wykrywania oraz usuwania metadanych z binarnych plików DOC. Nie obsługuje nowego formatu DOCX, lecz nowsze wersje Microsoft Office umożliwiają usunięcie metadanych przy pomocy Inspektora dokumentów. Alternatywnie można zapisać plik, z którego chcemy usunąć metadane w formacie binarnym DOC lub w formacie PDF.

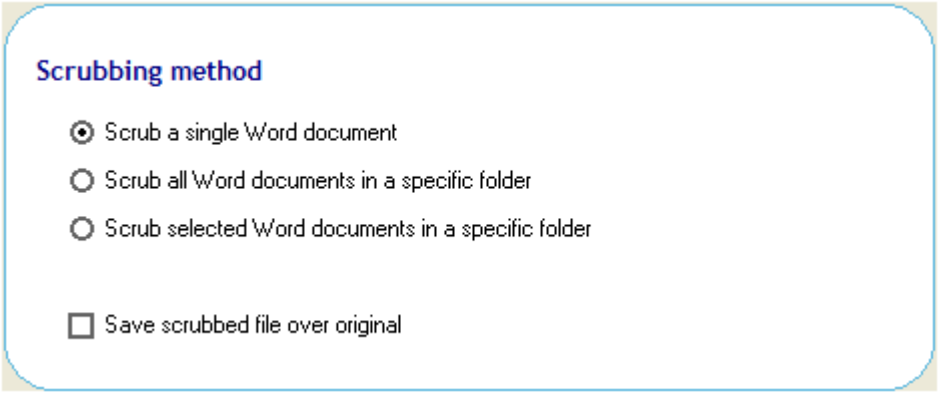
Ściągnij program Doc Scrubber ze strony producenta, firmy BrightFort http://www.brightfort.net/downloads/docscrubbersetup12.exe.

Zainstaluj program – przeczytaj i zaakceptuj warunki licencji (program jest bezpłatny do osobistego i edukacyjnego użytku). Program ma anglojęzyczny interfejs, lecz jest bardzo prosty w użyciu. Kliknij *Analyze* i wskaż plik DOC (kliknij *Browse*), który chcesz przeanalizować pod kątem zawartości metadanych. Następnie kliknij *Next* i w otwartym oknie zobaczysz wynik analizy metadanych.



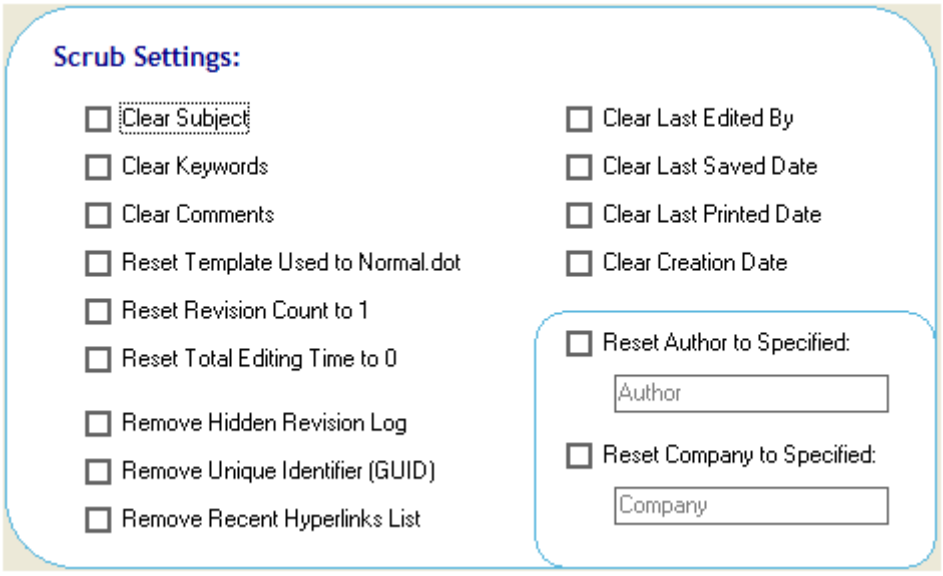
Wynik analizy można zapisać do pliku – kliknij *Save Log to File*.

Kliknij *Main Menu*, aby powrócić do głównego okna programu. Teraz możesz kliknąć *Scrub*, aby usunąć ze wskazanego pliku/ plików metadane. Masz do wyboru kilka opcji „czyszczenia" plików z metadanych.



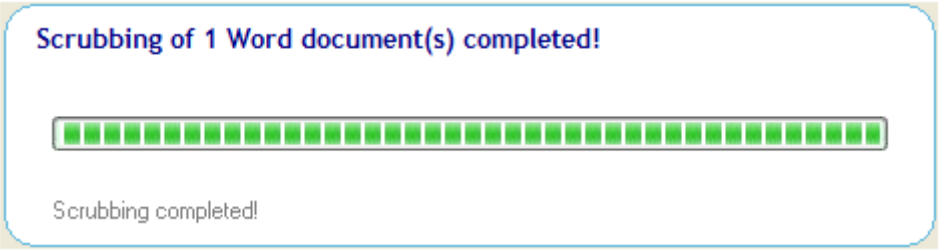
Domyślnie wybrana jest opcja dla pojedynczego dokumentu (*Scrub a single Word document*). Nie warto zaznaczać opcji *Save srubbed file over original,* ponieważ oryginalny plik zostanie nadpisany. Dostępne są również opcje „czyszczenia" (ang. scrub) wszystkich dokumentów (*Scrub all Word documents*) lub wybranych dokumentów (*Scrub selected Word documents*) w określonym folderze. (*in a specific folder*) Kliknij *Next* i wybierz plik (*Browse for file*) lub folder (*Browse for folder*).

Po wskazaniu pliku lub foldera kliknij ponownie *Next* i wybierz, jakie metadane mają być usunięte.

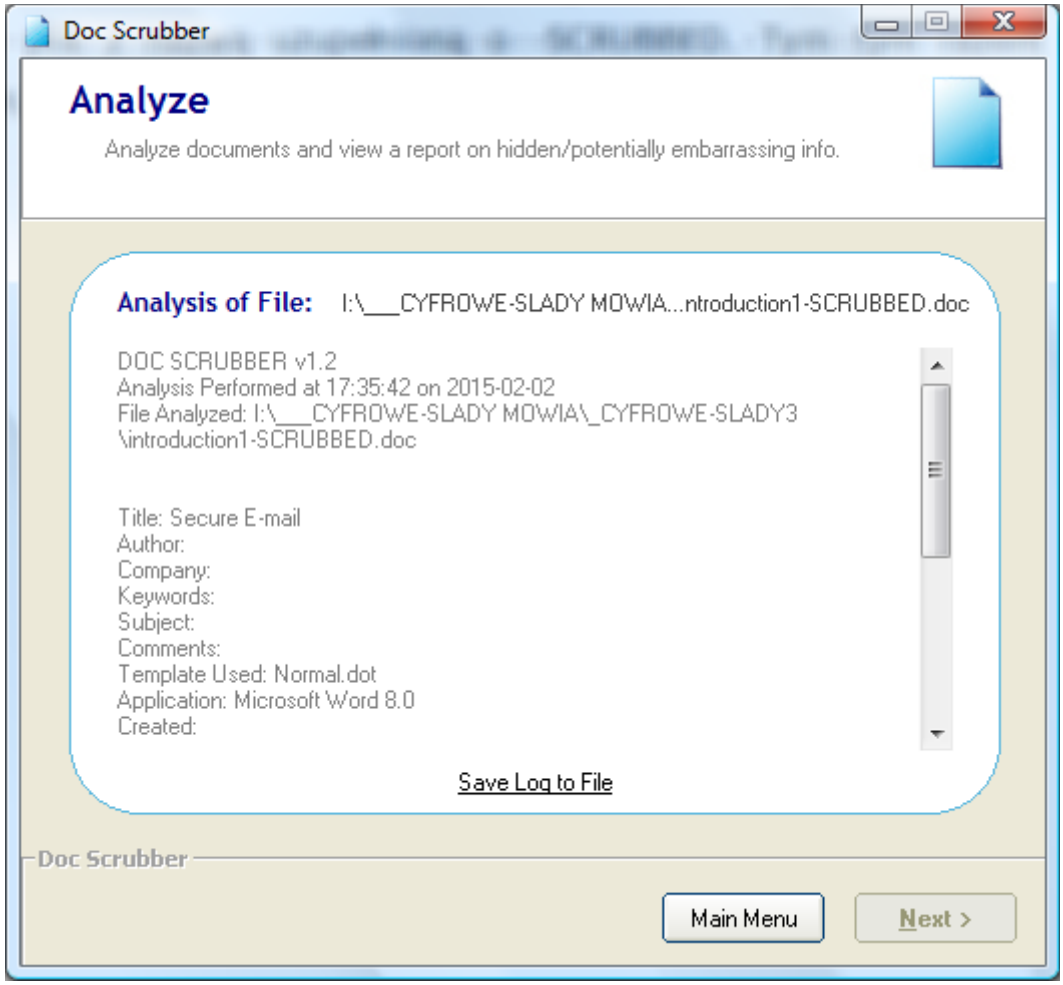


Można wybrać wszystkie pozycje (lub tylko te które chcemy usnąć) oraz zaznaczyć ponowny zapis (*Reset*) pola Firmy (*Company*) oraz Autora (*Author*) i wpisać wybrane nazwy lub pozostawić puste pola.

Następnie kliknij *Next* i po chwili pojawi się komunikat:

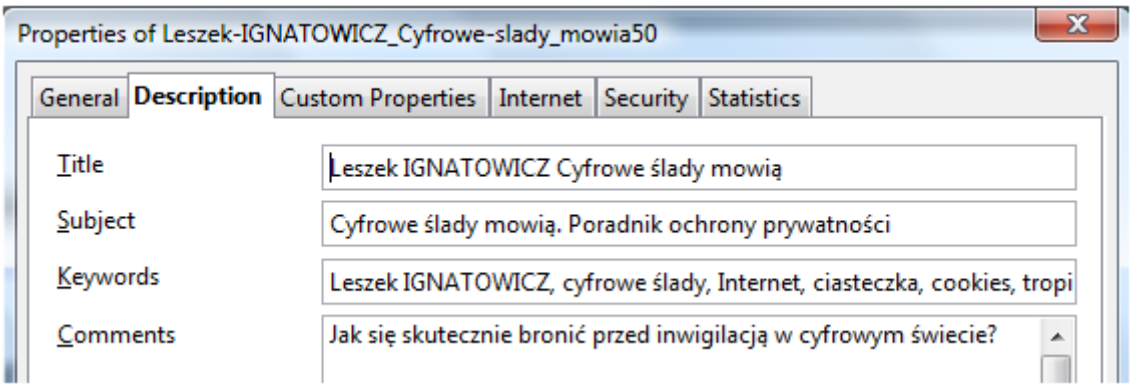


Można przeanalizować (kliknij *Analyze* w głównym oknie programu) „wyczyszczony” plik z nazwą uzupełnioną o -SCRUBBED. Tym razem zauważymy, że metadane zostały usunięte (poza polem *Title* – Tytuł, które pozostaje niezmienione).



Metadane w plikach Open Office

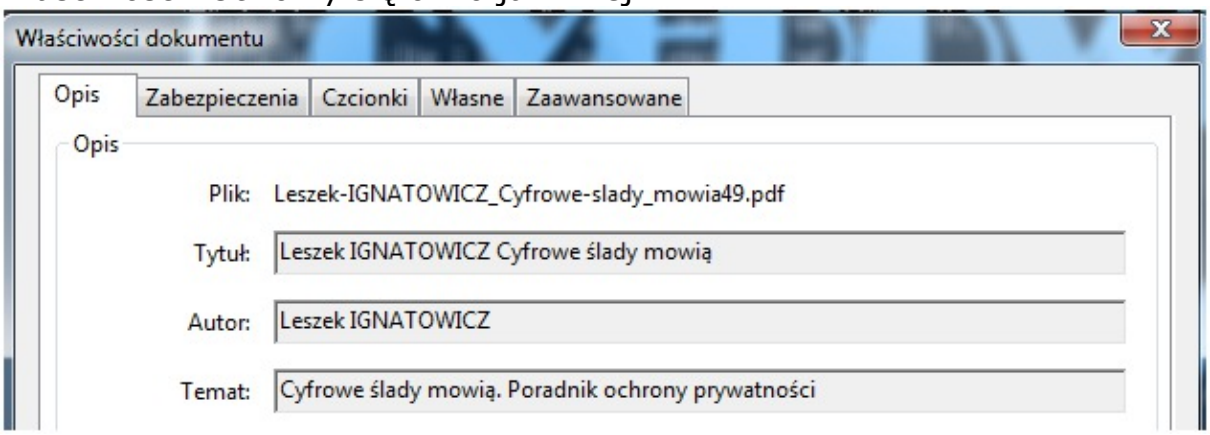
Dostępny bezpłatnie pakiet oprogramowania Open Office, konkurujący z Microsoft Office, również zapisuje metadane, lecz umożliwia ich edytowanie przy każdym zapisaniu pliku z użyciem *Zapisz jako*.



Open Office Writer, którego właśnie używam, umożliwia zapisanie tworzonego pliku w formacie PDF, do którego powyższe informacje są przynoszone jako metadane (przed wyeksportowaniem tworzonego dokumentu jako PDF metadane można dowolnie edytować lub usunąć).

Metadane w plikach PDF

Metadane w plikach PDF najłatwiej sprawdzić otwierając dokument w bezpłatnej aplikacji Adobe Reader. Wystarczy w menu *Plik* kliknąć *Właściwości*. Otworzy się okno jak niżej.

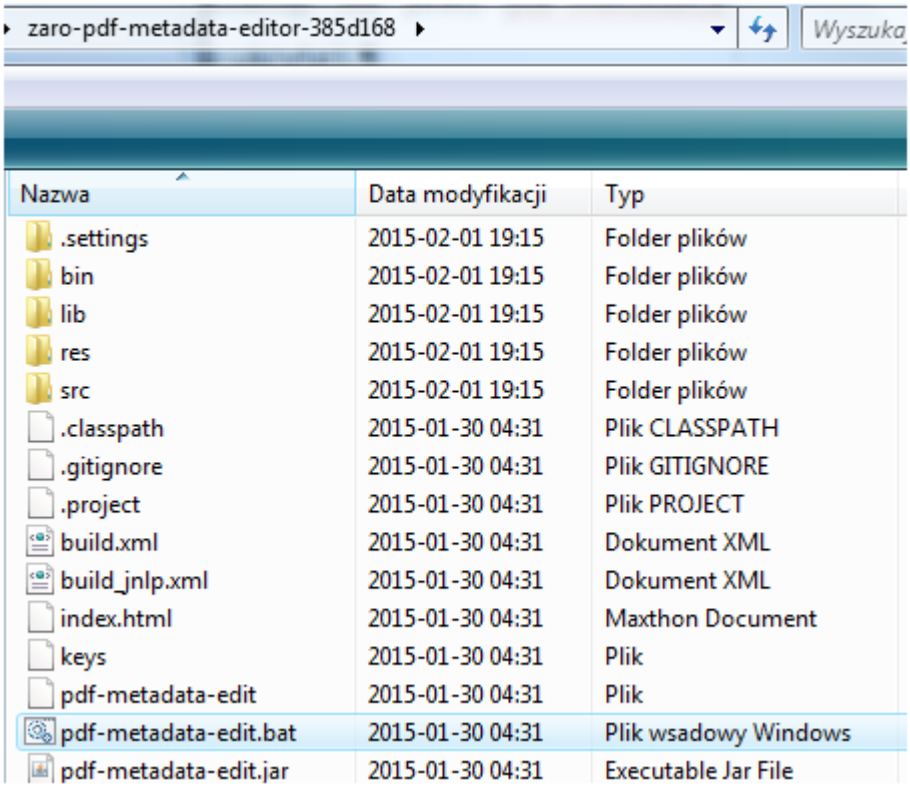


Usuwanie metadanych z plików PDF - PDF Metadata Editor

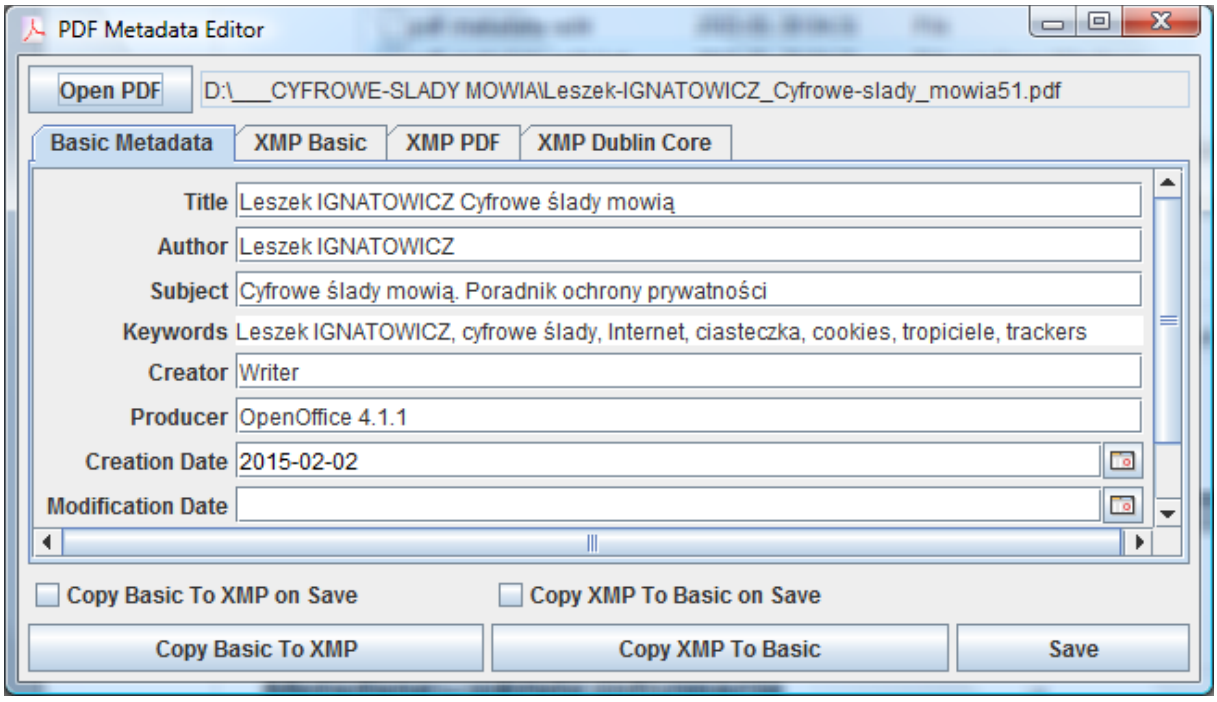
Metadane w plikach PDF można zmienić. Umożliwiają to komercyjne, płatne programy. Oczywiście, nie warto kupować oprogramowania, żeby zmienić czy też wykasować metadane w jednym lub kilku plikach PDF. I nie trzeba! Jest dostępny dobry, bezpłatny program PDF Metadata Edytor.

Ściągnij program ze strony twórcy http://zaro.github.io/pdf-metadata-editor/ (kliknij *Download*).

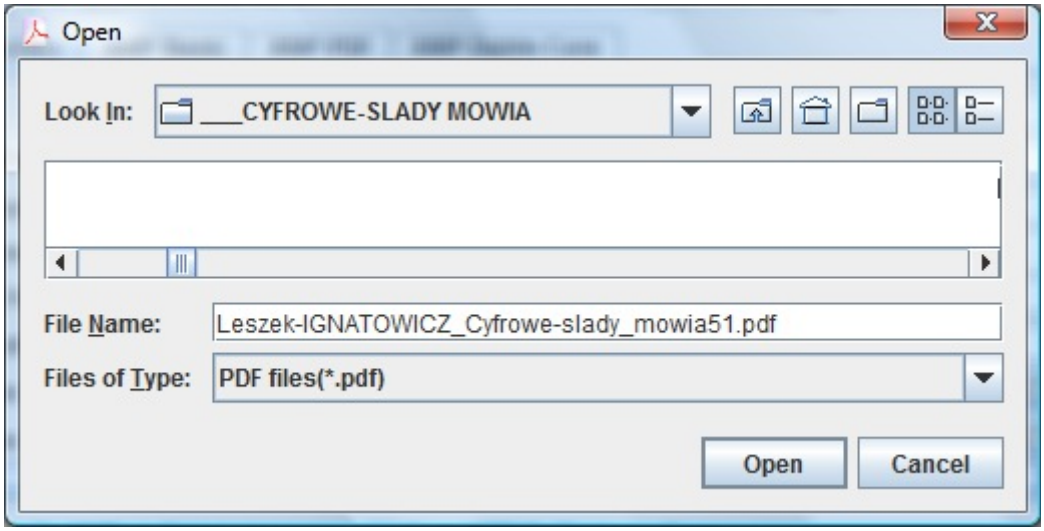
Program jest zawarty w archiwum zip. Nie wymaga instalacji. Wystarczy rozpakować plik *.zip w dogodnym miejscu na dysku twardym. Pojawi się folder *zaro-pdf-metadata-editor-385d168* z zawartością jak niżej. Aby uruchomić, program należy kliknąć na pliku pdf-*metadata-edit.bat* (rozszerzenie .bat jest domyślnie ukryte).



Program PDF Metadata Edytor jest napisany w języku Java, dlatego też do jego działania jest wymagana Java, zainstalowana w komputerze.



Używanie programu nie jest trudne. Wystarczy kliknąć *Open PDF,* wybrać plik do edycji metadanych i kliknąć *Open*.



Program umożliwia sprawdzenie, jakie metadane zawiera otwarty plik PDF (podobnie jak Adobe Reader) oraz dowolne ich zmodyfikowanie, w tym także usunięcie (skasuj zwartości pól, które chcesz usunąć).

Kliknij *x* w prawym górnym rogu okna programu, żeby go zamknąć bez modyfikowania metadanych pliku PDF. Natomiast jeśli chcesz trwale zmienić, czy też wykasować metadane kliknij *Save*.

Metadane w plikach graficznych/ zdjęciach JPEG

Pliki graficzne JPEG (rozszerzenie .jpg lub .jpeg) służą najczęściej do zapisu zdjęć, wykonywanych przy pomocy aparatów cyfrowych lub różnych urządzeń mobilnych, zwłaszcza smartfonów. W plikach tych, oprócz obrazu, czyli danych, zapisywanych jest mnóstwo dodatkowych informacji - metadanych. Są to najczęściej data i czas utworzenia pliku, typ użytego aparatu i jego ustawienia podczas robienia zdjęcia lub marka, model i operator smartfona, a czasem także położenie geograficzne miejsca utworzenia pliku.

Metadane w plikach JPEG noszą nazwę Exif (ang. Exchangeable Image File Format). Są przydatne w procesie przetwarzania, czy też katalogowania zdjęć. Mogą natomiast ujawniać zbyt dużo informacji, jeśli zostaną umieszczone w Internecie. Nawet te nieudostępnione publicznie, ponieważ - mimo zabezpieczeń - mogą zostać wykradzione. Szczególnie niebezpieczne może być ujawnienie danych geolokalizacji miejsca wykonania zdjęcia. Przykład poniżej (smartfon Apple, iPhone 5):

```
---- GPS ----
GPS Latitude Ref                : North
GPS Latitude                    : 39 deg 17' 14.40"
GPS Longitude Ref               : West
GPS Longitude                   : 76 deg 36' 36.60"
GPS Altitude Ref                : Above Sea Level
GPS Altitude                    : 30 m
GPS Time Stamp                  : 04:02:56.95
GPS Img Direction Ref           : True North
GPS Img Direction               : 256.0428135
```

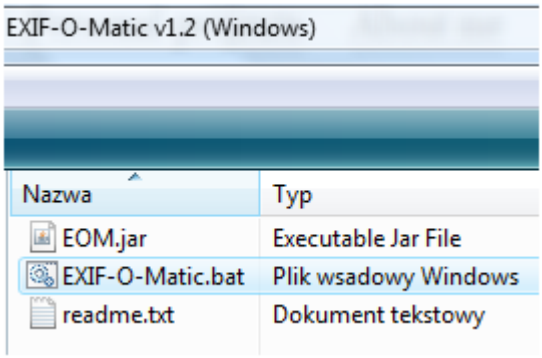
Może warto wyłączyć geolokalizację - zobacz How to Disable Geotagging on Your Smartphone's Camera (Android, iPhone, BlackBerry).

Analiza metadanych w plikach JPEG – program Exif-O-Matic

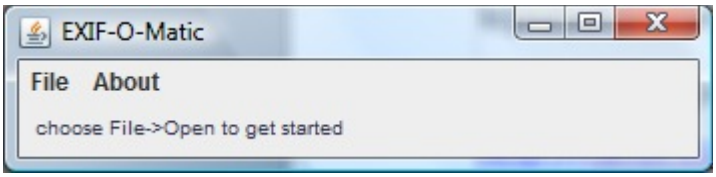
Podstawowe informacje Exif można sprawdzić bezpośrednio w systemie Windows – kliknij prawym klawiszem myszy na pliku, a następnie wybierz *Właściwości* oraz zakładkę *Szczegóły*. W celu sprawdzenia całej zwartości Exif należy użyć dodatkowego oprogramowania. Mogą to być programy graficzne, w tym bezpłatny IrfanView. Są także wyspecjalizowane programy do analizy metadanych Exif. Jednym z lepszych i łatwych w użyciu jest bezpłatny Exif-O-Matic.

Ściągnij program Exif-O-Matic for Windows ze strony twórcy http://rahul.connectionlab.org/personal-projects/exif-o-matic/.

Napisany w języku Java program nie wymaga instalacji. Po prostu rozpakuj ściągnięty plik *EXIF-O-Matic-Windows.zip* w dogodnym miejscu na dysku komputera i otwórz folder jak niżej.

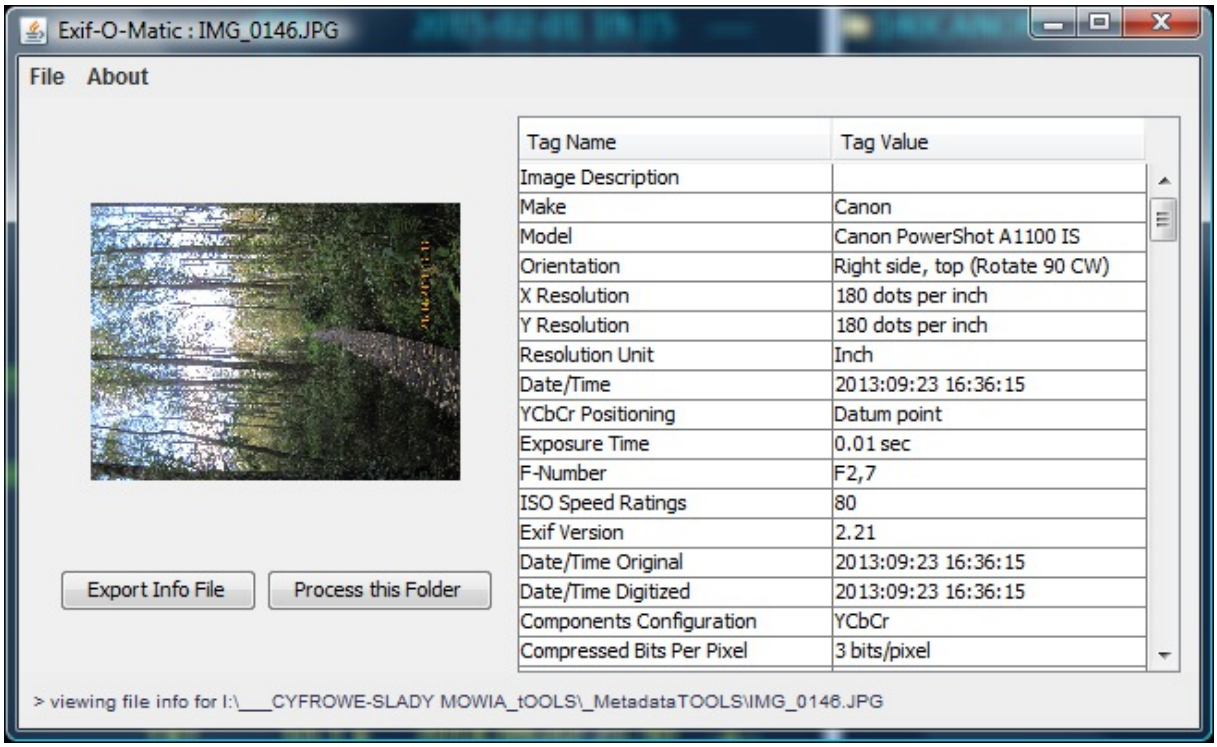


Uruchomienie programu następuje po kliknięciu pliku EXIF-O-Matic.bat (rozszerzenie .bat jest domyślnie niewidoczne). W komputerze powinna być zainstalowana Java (najczęściej jest zainstalowana, chociaż nie jest składnikiem systemu Windows). Otworzy się okno jak niżej.



Kliknij *File*, a następnie *Open* i wybierz plik JPEG, którego metadane chcesz przeanalizować.

A oto przykład analizy zdjęcia ze zbiorów autora:

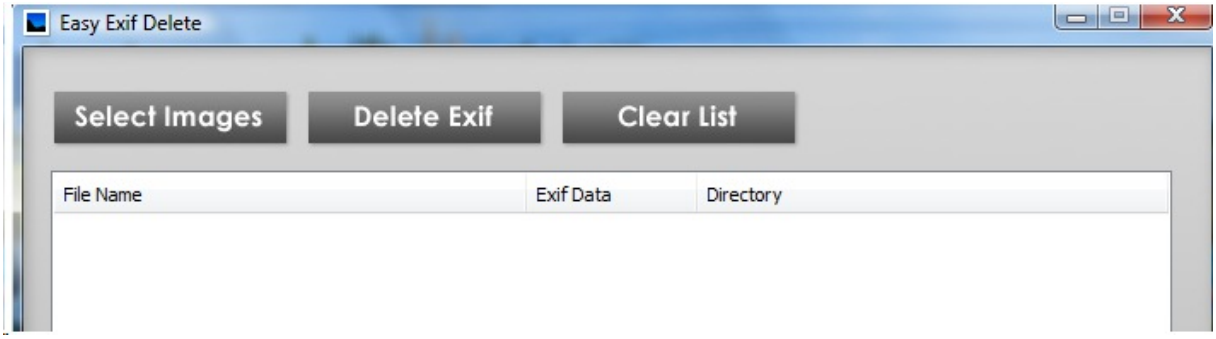


Uzyskane informacje Exif można wyeksportować do pliku .txt lub .html – w tym celu kliknij *Export Info File*. Natomiast przycisk *Process this Folder* umożliwia przeanalizowanie wszystkich plików JPEG w folderze, z którego pochodzi badane zdjęcie i zapisanie zbiorczego raportu. Następnie raport należy otworzyć i sprawdzić, jakie pliki zawierają metadane Exif. Na tej podstawie można zadecydować, czy należy te metadane usunąć, zanim te pliki zostaną udostępnione.

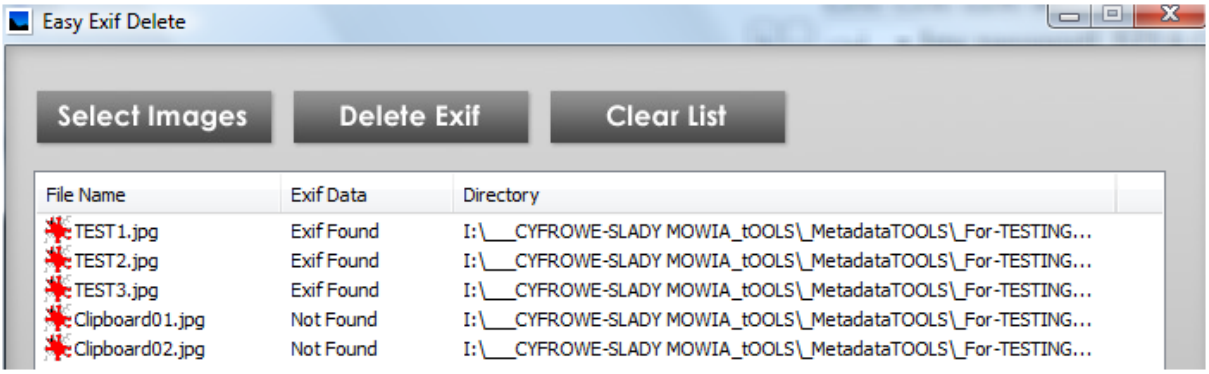
Usuwanie metadanych Exif z plików JPEG - Easy Exif Delete

Zdjęcia i inne pliki JPEG, które chcemy umieścić w Internecie, powinny być pozbawione metadanych Exif. Służy do tego celu bezpłatny program Easy Exif Delete.

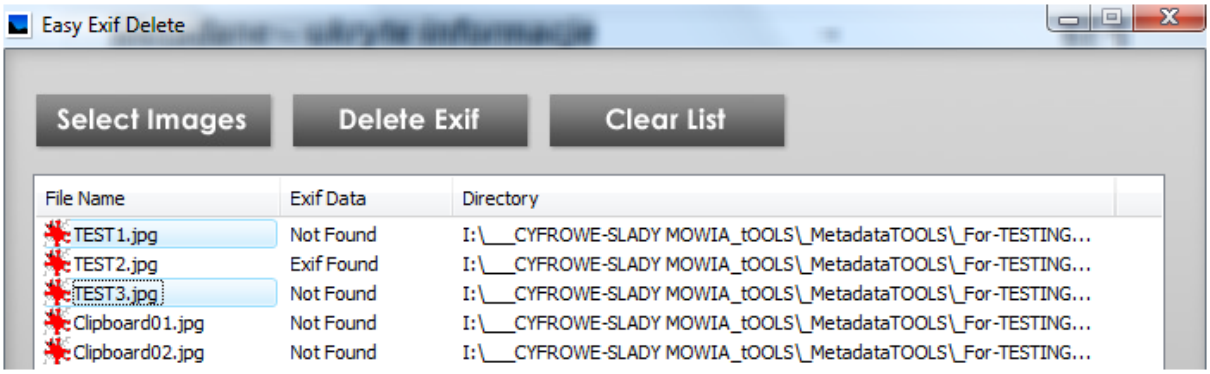
Ściągnij program ze strony producenta firmy, ConsumerSoft http://www.easyexifdelete.com/. Zainstaluj program, tak jak każdą typową dla systemów Windows aplikację i uruchom.



Obsługa programu jest łatwa. Kliknij *Select Images* (Wybierz Obrazy) i wskaż pliki zdjęć, posługując się w typowy sposób klawiszami *Shift* oraz *Ctrl* w celu ich zaznaczenia. Następnie kliknij *Otwórz* i wybrane pliki zostaną przeanalizowane. Te, w których występują metadane Exif, zostaną oznaczone komunikatem *Exif Found* (Znaleziono Exif).



W oknie programu, jak wyżej, zaznacz te pliki, z których chcesz usunąć metadane Exif i kliknij przycisk *Delete Exif*. Po wykonaniu tej operacji pliki w kolumnie *Exif Data* zostaną oznaczone *Not Found* (Nie znaleziono).



Program usuwa metadane Exif, nie zapisując kopii oryginałów! Przycisk *Clear List* (Wyczyść listę) usuwa z okna programu wyświetlane pliki. Można wybrać kolejne pliki do wykrywania i czyszczenia danych Exif.

Prywatność czy anonimowość?

Na zakończenie tego poradnika warto zastanowić się nad relacją prywatności i anonimowości w Internecie. Może to jest to samo lub prawie to samo? Oba określenia są trochę zbliżone, lecz z pewnością nie są tożsame. Można powiedzieć, że anonimowość gwarantuje zachowanie prywatności, lecz nie odwrotnie.

Omówione w poradniku sposoby ochrony prywatności również są elementarzem zachowania anonimowości. W większości przypadków skutecznie utrudnią identyfikację użytkownika. Na tyle skutecznie, że uniemożliwią profilowanie, wykrycie autora wpisu na forum, autora innej typowej aktywności internetowej. Natomiast nie zapewnią anonimowości w przypadku, gdy wyspecjalizowane służby, z jakichkolwiek powodów, podjęły działania mające na celu inwigilację użytkownika. Dlaczego? Nie chodzi tylko o niewystarczające środki techniczne. Aczkolwiek jeżeli nie stosujemy fałszowania adresu sprzętowego (ang. MAC address spoofing) karty sieciowej, za pomocą której łączymy się z Internetem, możliwa jest identyfikacja komputera lub urządzenia mobilnego. W tym miejscu przestrzegam, że zmiana adresu MAC może spowodować utrudnienia w dostępie, a nawet odłączenie od Internetu.

Zachowanie anonimowości w Internecie wymaga stosowania wyrafinowanych środków technicznych oraz ścisłego przestrzegania procedur bezpieczeństwa (ang. opsec). Okazuje się, że analiza przyczyn deanonimizacji najbardziej poszukiwanych administratorów serwisów *ukrytych w sieci Tor* (np. Silk Road) wykazała, że nie zawiodły środki techniczne, lecz przyczyną było nieprzestrzeganie opsec. Ale o tym w innym poradniku, który zostanie opublikowany niebawem...

Źródła, ebooki, zasoby online

Źródła:

Peter Loshin „Practical Anonymity. Hiding in Plain Sight Online”,

© 2013 Elsevier, Inc.

Doug Lowe „Networking All-in- One For Dummies”,

© 2013 by John Wiley & Sons, Inc.

John Sammons *„The Basics of Digital Forensics”*, © 2012 Elsevier, Inc.

The SSD Project, Surveillance Self-Defense, *https://ssd.eff.org/*

What can I do to prevent being tracked when reading the news online?,

https://myshadow.org/trackography-solutions

Ebooki:

Leszek IGNATOWICZ, „Cyfrowe ślady. Jest się czego bać”, 2014

Do bezpłatnego pobrania z Internetu *http://pdf.helion.pl/s_5602/s_5602.pdf*

Leszek IGNATOWICZ, „Odkryj ukryty Internet. Jak używać sieci Tor”,

w opracowaniu

Zasoby online:

Electronic Frontier Foundation

Fundacja Panoptykon

Your IP address, Country, ISP, Browser and other details

BrowserSpy.dk