Laboratorium 1

Wprowadzenie do steganografii. Specjalistyczne oprogramowanie.

1. Praca z zasobami steganografii online

1. Rejestracja na platformach online: Uzyskaj dostęp do platform online do steganografii, takich jak https://georgeom.net/StegOnline/upload, https://stylesuxx.github.io/steganography/ lub innych.

2. Pobieranie plików: Załaduj różnorodne pliki multimedialne na wybrane platformy online. Wybierz pliki różnych formatów, takie jak obrazy (JPEG, PNG, BMP), pliki dźwiękowe (MP3, WAV) oraz wideo (AVI, MP4).

3. Ukrywanie informacji: Korzystając z funkcji wybranych platform online, ukryj wiadomości tekstowe w plikach multimedialnych. Wypróbuj różne metody ukrywania proponowane przez te platformy.

4. Analiza wyników: Przejrzyj utworzone pliki steganograficzne i ocen ich wygląd zewnętrzny lub jakość dźwięku/obrazu. Sprawdź, czy można zauważyć obecność ukrytych informacji bez specjalnego dekodowania.

5. Odzyskiwanie ukrytych informacji: Korzystając z tych samych platform online, spróbuj odzyskać ukryte informacje z utworzonych plików steganograficznych. Oceń skuteczność różnych metod odzyskiwania.

6. Analiza porównawcza: Porównaj wyniki korzystania z różnych platform online do steganografii. Oceń ich wygodę, szybkość i skuteczność działania.

7. Tworzenie raportu: Przygotuj raport zawierający wyniki Twojej pracy, w tym opis wykonanych działań, szczególne cechy różnych platform online oraz Twoje wnioski dotyczące ich użyteczności.

1. Praca z narzędziami S-Tools.

**Wprowadzenie do S-Tools**

S-Tools to wszechstronne i potężne narzędzie steganograficzne używane do ukrywania informacji w plikach cyfrowych, głównie obrazów i plików dźwiękowych.

Steganografia to praktyka ukrywania jednego kawałka danych (ukrytej wiadomości) w innym (nośniku) w taki sposób, aby było to trudne do wykrycia.

S-Tools osiąga to poprzez subtelne zmienianie najmniej istotnych bitów (LSB) pliku nośnika, aby osadzić ukryte dane bez zauważalnego wpływu na wizualną lub słyszalną jakość nośnika.

S-Tools obsługuje głównie formaty obrazów takie jak JPEG, BMP i GIF, a także formaty dźwiękowe takie jak WAV.

W tym kompleksowym przewodniku zagłębimy się w różne aspekty S-Tools, w tym jego funkcje, zastosowanie i kwestie etyczne.

Czym jest steganografia obrazów?

Steganografia obrazów to technika używana do ukrywania tajnych informacji lub wiadomości w cyfrowych obrazach bez widocznej zmiany wyglądu obrazu. Pozwala to na tajną komunikację i może być używane do różnych celów, takich jak bezpieczny transfer danych czy szyfrowanie.

Najczęstszą metodą w steganografii obrazów jest zmiana najmniej istotnych bitów (LSB) wartości pikseli. Poprzez subtelne zmiany w tych najmniej istotnych bitach, ukryte dane są włączane do obrazu.

Steganografia obrazów za pomocą S-Tools

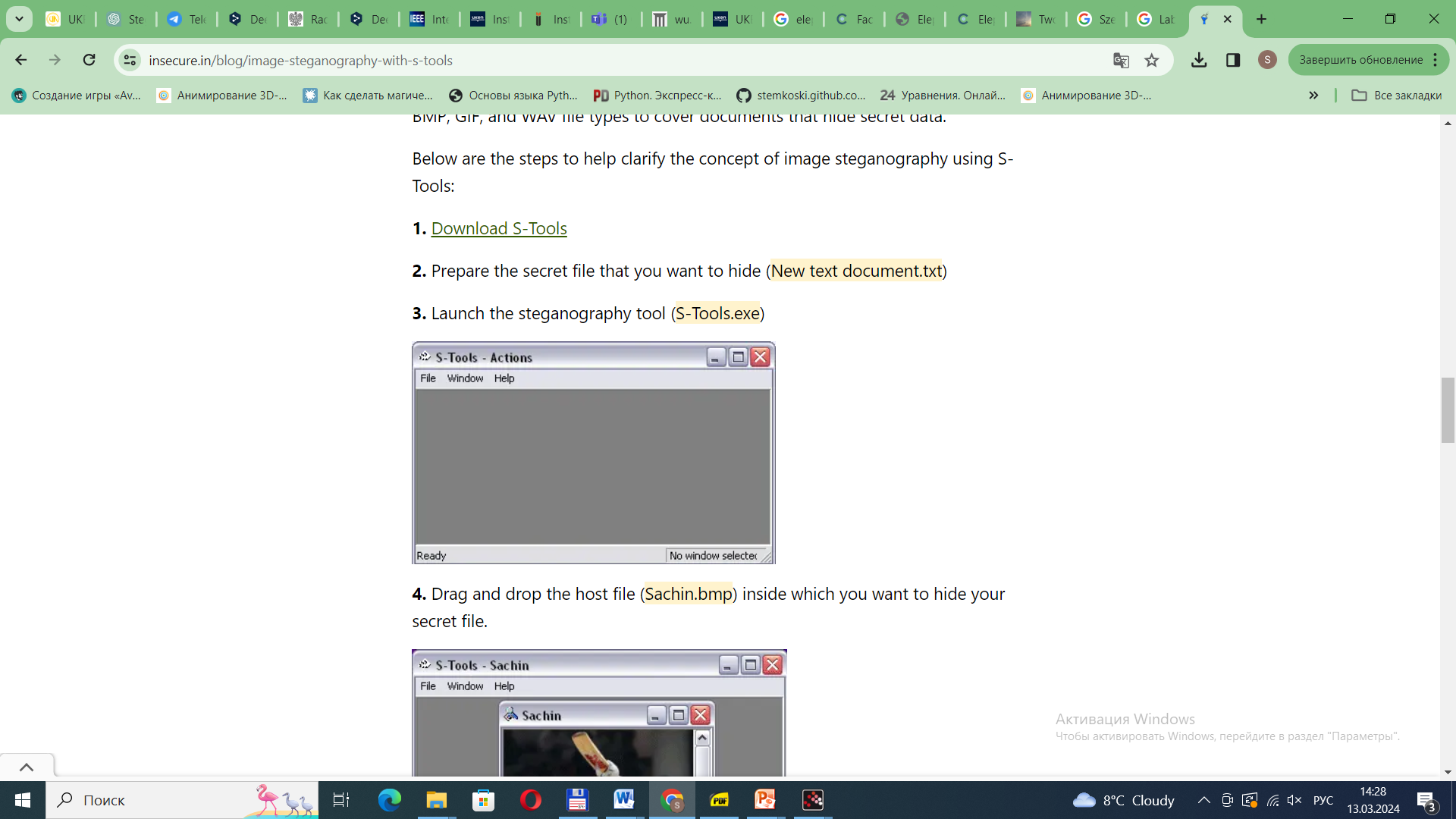
S-Tools to narzędzie steganograficzne opracowane przez Andy'ego Browna. S-Tools ukrywa tajną wiadomość w pliku okładki za pomocą losowo dostępnych bitów. Możesz użyć typów plików BMP, GIF i WAV do okładki dokumentów ukrywających tajne dane.

Poniżej przedstawiamy kroki, które pomogą zrozumieć koncepcję steganografii obrazów za pomocą S-Tools:

1. Pobierz S-Tools.

2. Przygotuj plik tajny, który chcesz ukryć (Nowy dokument tekstowy.txt).

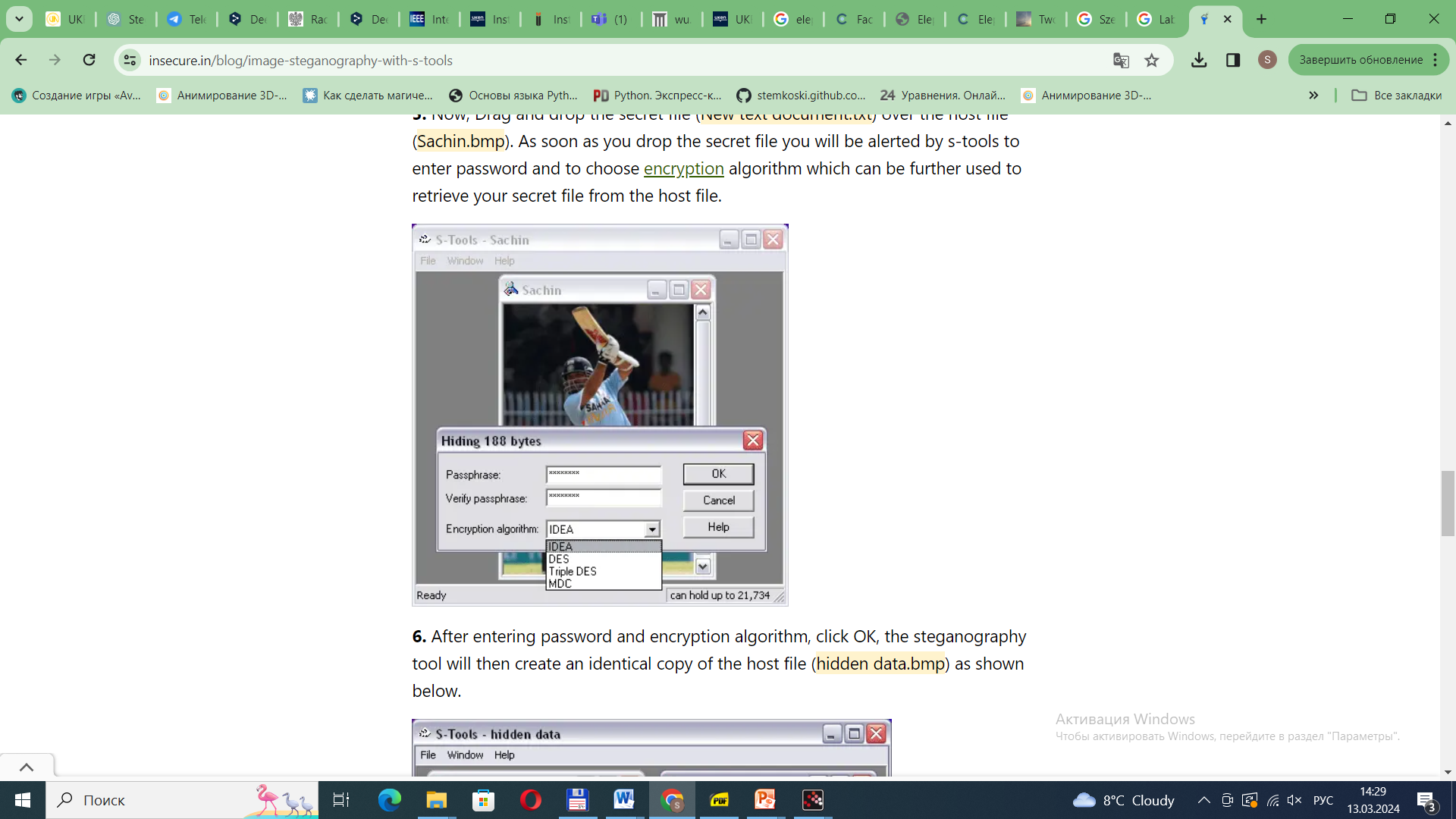
3. Uruchom narzędzie steganograficzne (S-Tools.exe).



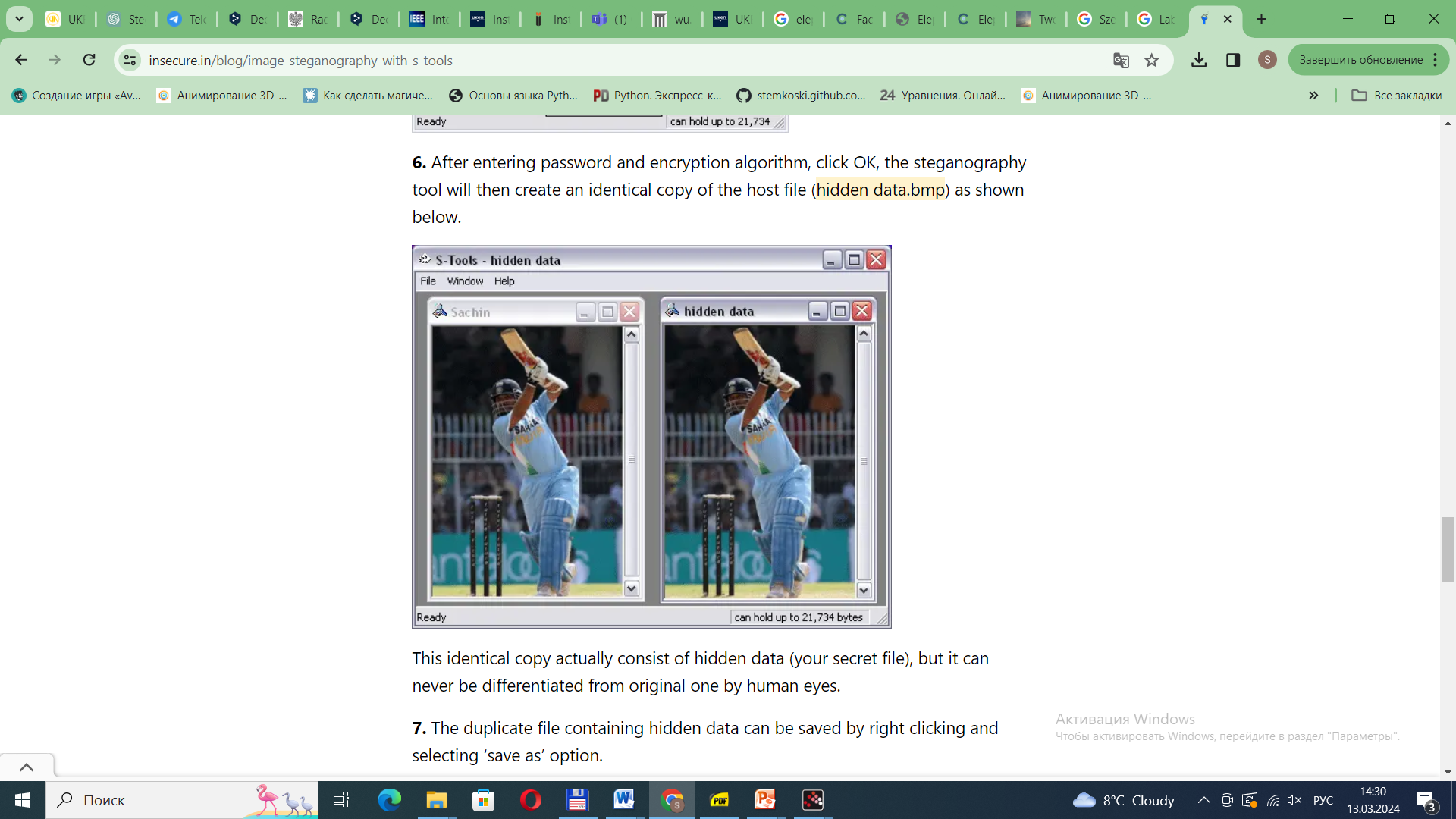
4. Przeciągnij i upuść plik nośnika (Sachin.bmp), w którym chcesz ukryć swój plik tajny.



5. Teraz przeciągnij i upuść plik tajny (Nowy dokument tekstowy.txt) na plik nośnika (Sachin.bmp). Gdy tylko upuścisz plik tajny, zostaniesz poinformowany przez S-Tools, aby podać hasło i wybrać algorytm szyfrowania, który można dalej użyć do odzyskania pliku tajnego z pliku nośnika.



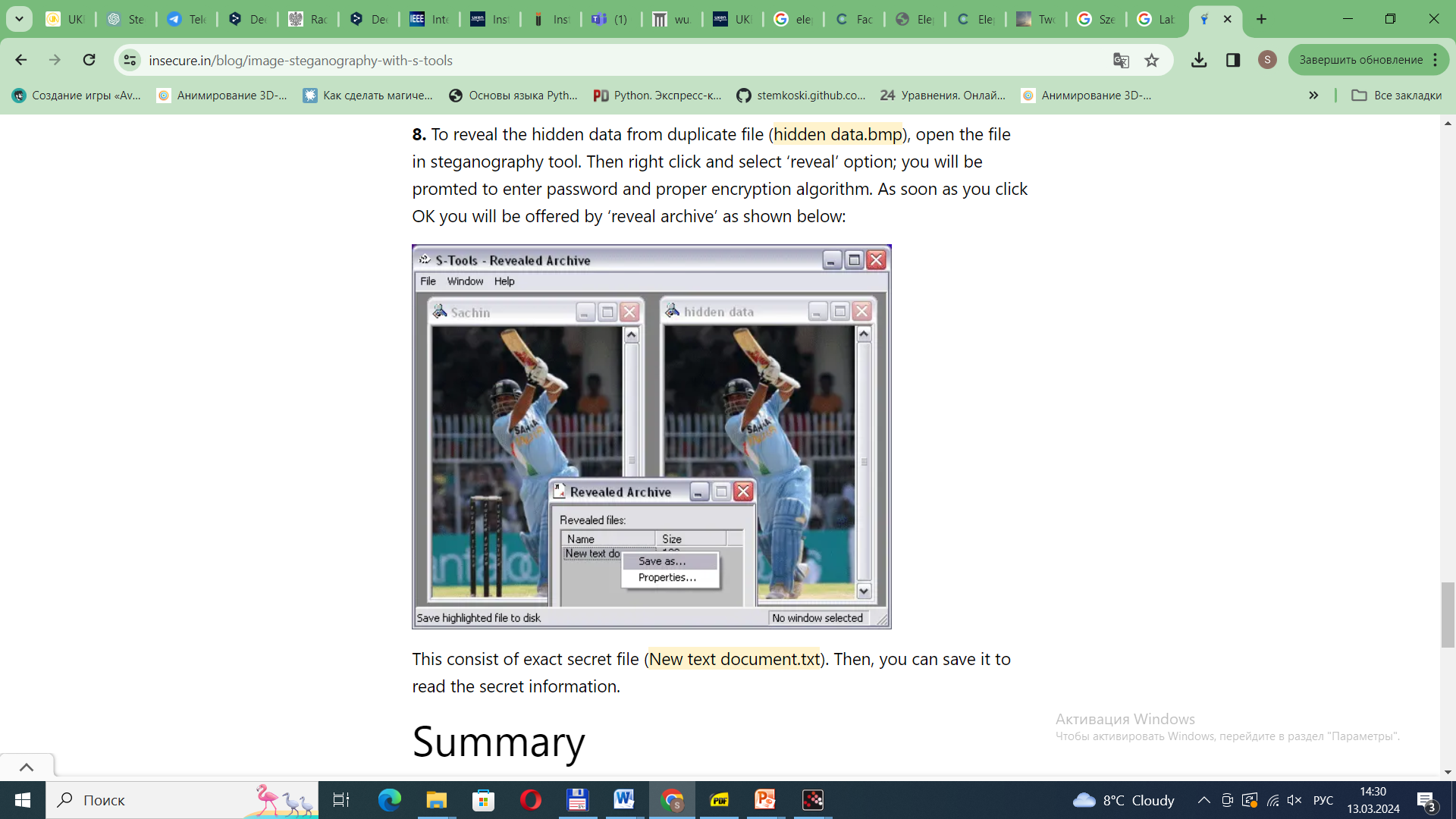
6. Po wprowadzeniu hasła i algorytmu szyfrowania kliknij OK, a narzędzie steganograficzne utworzy identyczną kopię pliku nośnika (ukryte dane.bmp), jak pokazano poniżej.



7. Ta identyczna kopia faktycznie zawiera ukryte dane (twój plik tajny), ale nigdy nie można jej odróżnić od oryginalnej przez ludzkie oczy.

8. Plik z duplikatem zawierającym ukryte dane można zapisać, klikając prawym przyciskiem myszy i wybierając opcję „Zapisz jako”.

9. Aby ujawnić ukryte dane z duplikatu (ukryte dane.bmp), otwórz plik w narzędziu steganograficznym. Następnie kliknij prawym przyciskiem myszy i wybierz opcję „ujawnij”; zostaniesz poproszony o podanie hasła i właściwego algorytmu szyfrowania. Gdy tylko klikniesz OK, zostaniesz poproszony o „ujawnienie archiwum”, jak pokazano poniżej:



To zawiera dokładny plik tajny (Nowy dokument tekstowy.txt). Następnie możesz go zapisać, aby przeczytać tajne informacje.

Podsumowanie

Możesz użyć S-Tools do ukrywania prywatnych lub poufnych informacji, których nie chcesz, aby wpadły w niepowołane ręce. Alternatywnie możesz użyć S-Tools do potwierdzenia swoich praw autorskich do obrazu lub dźwięku, przechowując w nim zaszyfrowane oświadczenie o prawach autorskich i wydobywając je w przypadku sporu.

Steganografia może być potężnym narzędziem do ochrony i ukrywania danych, gdy jest stosowana odpowiedzialnie i etycznie. Zawsze rozważaj implikacje prawne i etyczne przed zastosowaniem technik steganograficznych. S-Tools, dzięki swojemu przyjaznemu dla użytkownika interfejsowi i różnorodnym funkcjom, może być cennym narzędziem dla tych, którzy chcą wykorzystać steganografię w celach legalnych.