

CyberChef

CERT.hr-PUBDOC-2019-8-386

Sadržaj

1	UVOD	3
2	INSTALACIJA ALATA CYBERCHEF	4
3	KORIŠTENJE ALATA CYBERCHEF	5
3.1	HEXDUMP	5
3.2	BASE64	7
3.3	HTML	8
3.4	KODIRANJE ZNAKOVA	9
3.5	JSON	11
3.6	PGP	13
3.7	PARSE USER AGENT	14
3.8	PARSE IP RANGE	15
3.9	PARSE DATETIME	16
3.10	ANALYSE HASH	16
3.11	DETECT FILE TYPE.....	17
3.12	EXIF	18
4	ZAKLJUČAK	20

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT-a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

1 Uvod

„CyberChef“ je intuitivna web aplikacija namijenjena obradi digitalnih podataka koja omogućuje brzo i jednostavno pretvaranje podataka u različite formate, neka jednostavna kodiranja (Base64 ...), ali i složenije enkripcije (PGP ...), sažimanja i različite aritmetičke i logičke operacije.

Prednost ovog alata je to što omogućava primjenu raznih kompleksnih algoritama na način koji je jednostavan i intuitivan za korištenje čak i korisnicima s manje tehničkih znanja. Tako je na jednom mjestu dostupan veliki broj operacija koje je moguće izvršavati nad željenim podacima, nakon čijeg se unosa može odjednom zadati kombinacija više različitih pretvorbi, koje će dati konačni rezultat.

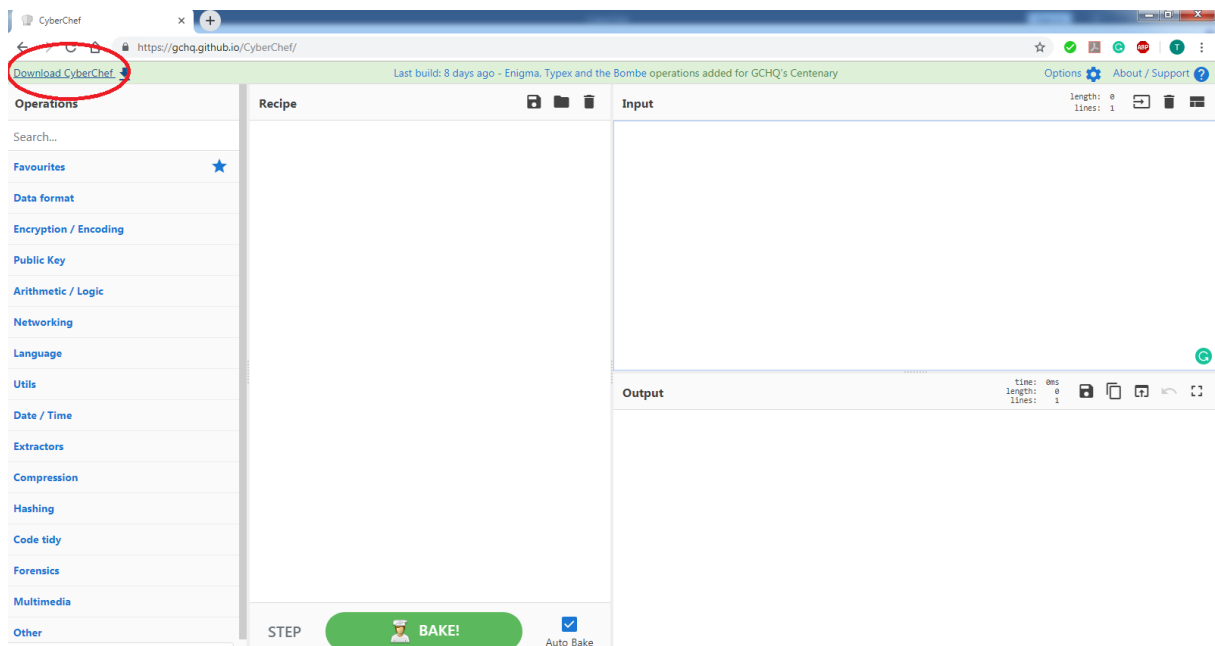
Korisničko sučelje napravljeno je na način koji osigurava lako korištenje različitih i mnogobrojnih alata: *drag-and-drop* principom slaže se željena funkcija, tzv. „recept“, koja se potom primjenjuje na ulazne podatke, a dobiveni izlaz ispisuje se u posebnom polju.

2 Instalacija alata CyberChef

Pri korištenju ovog alata nije potrebno raditi klasičnu instalaciju, već je moguće koristiti alat izravno preko [web stranice](#).

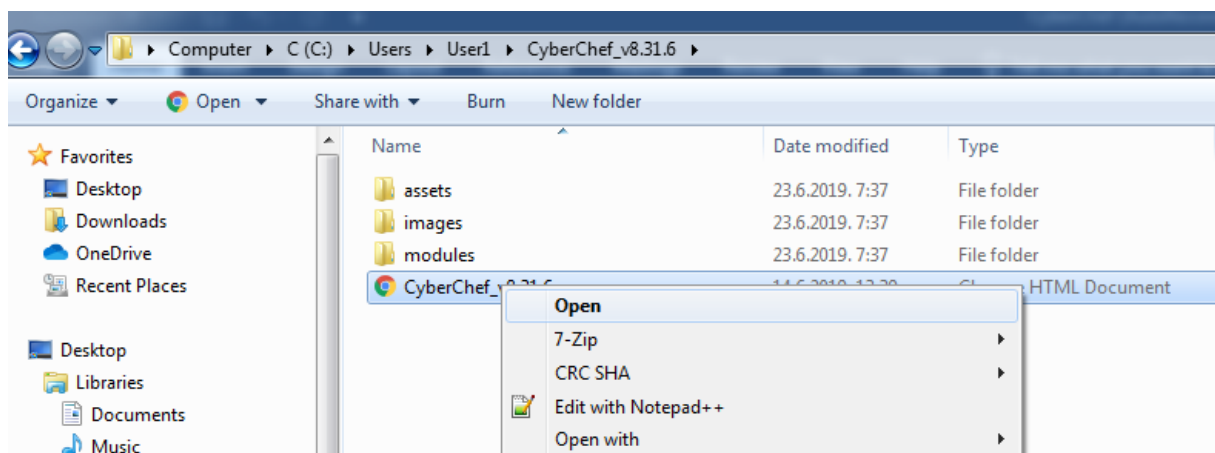
Postoji i mogućnost preuzimanja aplikacije za lokalno pokretanje na vlastitom računalu za slučaj da ju korisnik želi koristiti i kad nije spojen na mrežu, ili kad mu je važna privatnost podataka koje obrađuje i ne želi ih slati na tuđi poslužitelj.

U tom slučaju potrebno je preuzeti zip arhivu „CyberChefa“ klikom na „Download CyberChef“.



Slika 1. Preuzimanje „CyberChef“ aplikacije

Potom je datoteku potrebno raspakirati arhivu i pokrenuti „CyberChef“ HTML datoteku u nekom web pregledniku.



Slika 2. Pokretanje aplikacije

3 Korištenje alata CyberChef

Sučelje alata sastoji se od nekoliko glavnih polja: „Operations“ u kojem se biraju željene operacije za izvršavanje, „Recipe“ gdje se *drag and dropom* (povlačenjem i ispuštanjem klikom miša) kreira algoritam operacija, „Input“ gdje se upisuje ulazna poruka, a rezultat se ispisuje u polju „Output“.

U polju „Operations“ moguće je pretraživati nazive raspoloživih operacija pomoću polja za pretragu, što je vrlo praktično, s obzirom na velik broj dostupnih operacija/alata. Često korištene alate može se spremati u „Favorites“, kako ih se ne bi trebalo tražiti svaki put iznova. Stvorene „recepte“ također je moguće spremati i kasnije ih koristiti.

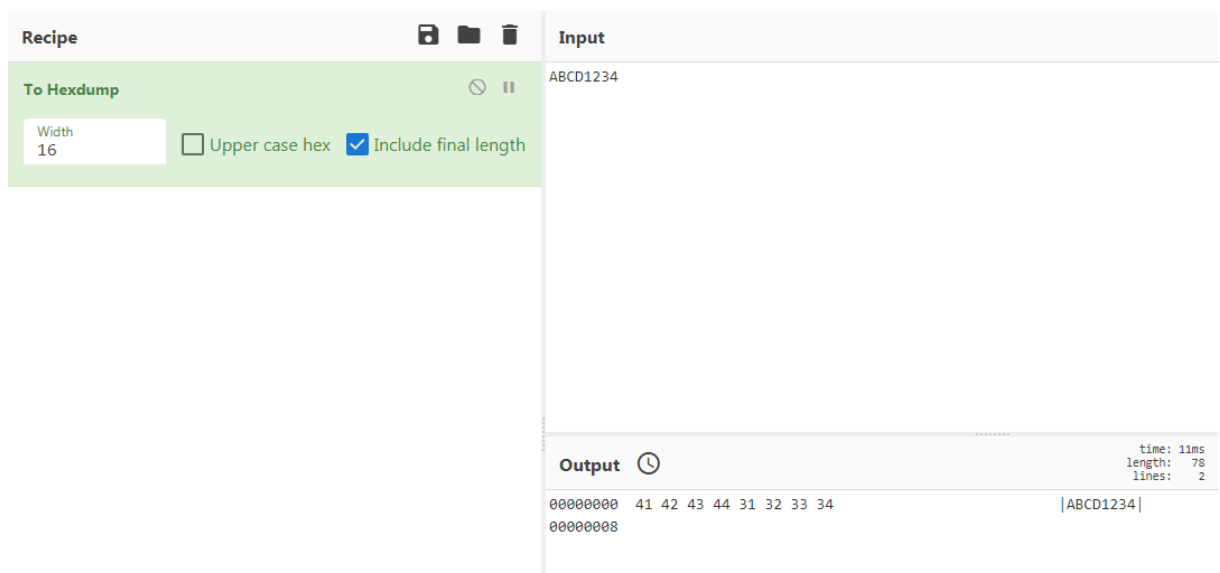
Izlazni podaci stvaraju se pritiskom na gumb „Bake“, a može se uključiti i opcija „Auto Bake“ za automatsku promjenu rezultata, ovisnu o promjeni bilo ulazne poruke bilo „recepta“.

U nastavku su navedeni neki alati i opisani načini njihova korištenja.

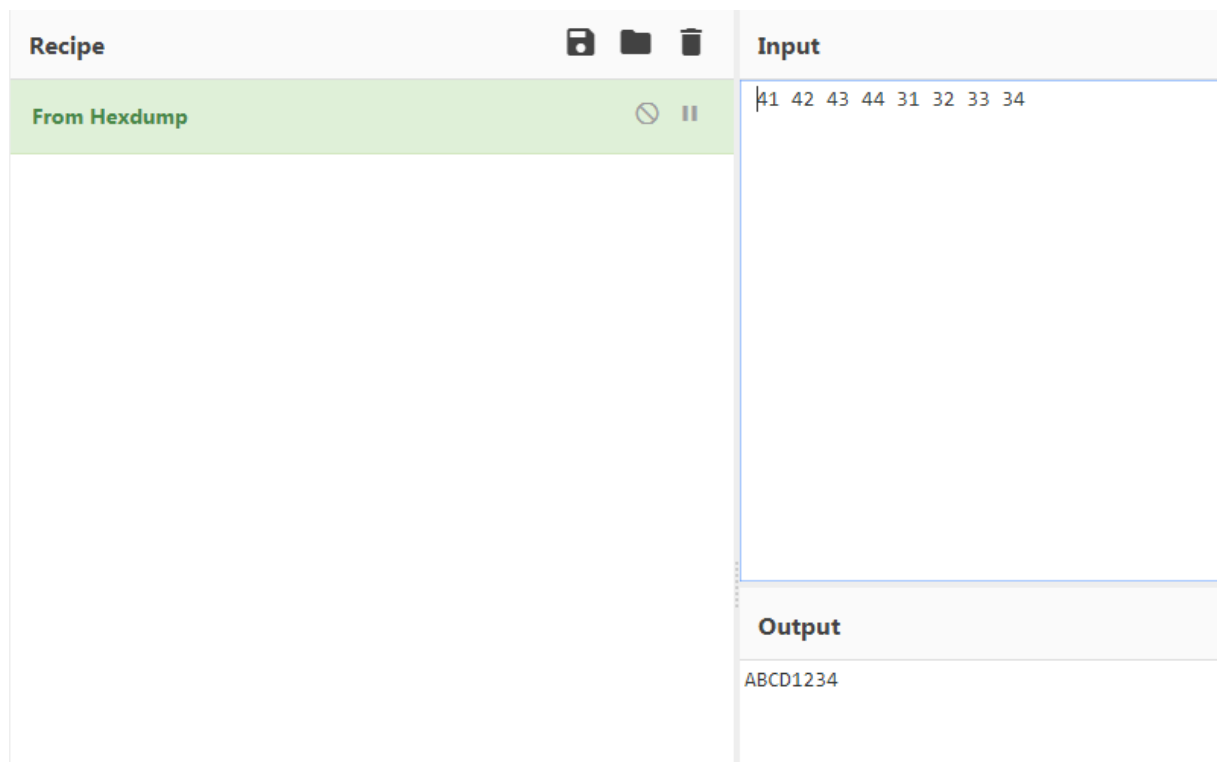
3.1 Hexdump

Opcijom „to Hexdump“ dobiva se heksadekadska i ASCII vrijednost svakog unesenog bajta, odijeljena razmakom. Ovakva pretvorba koristi se u *debugiranju* i reverznom inženjeringu. Pogodna je za npr. analizu velikog skupa binarnih podataka kako bi postao čitljiviji, a u slučaju datoteke sa znakovima koje nije moguće ispisati, olakšava rekonstrukciju podataka.

Alat nudi i suprotnu opciju „from Hexdump“ kojom se podaci vraćaju u izvorni oblik. Uz to, da bi pretvorio podatke u početni oblik, potrebno je niz započeti razmakom.

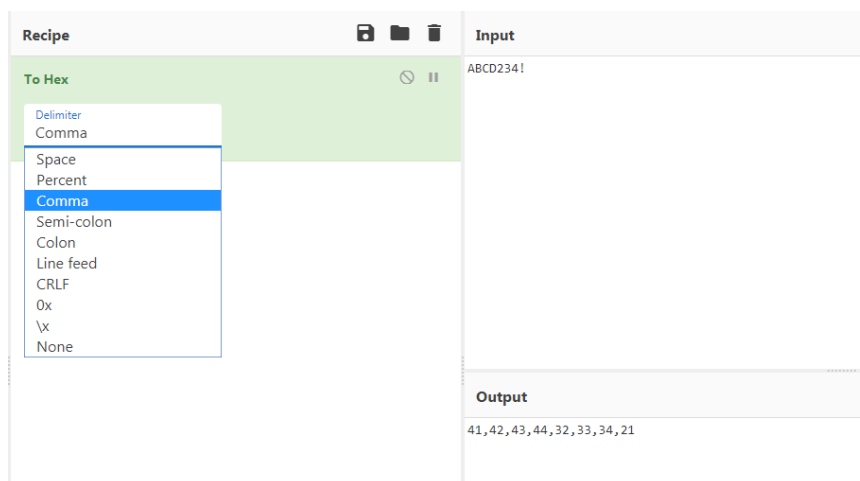


Slika 3. Pretvaranje u hexdump oblik

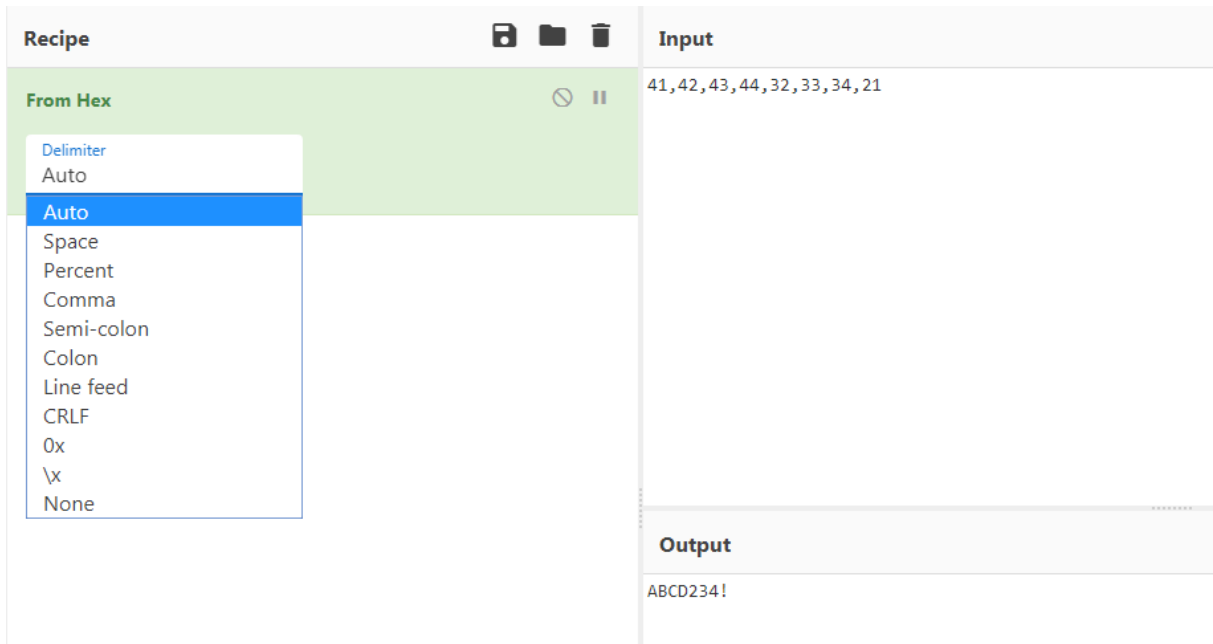


Slika 4. Pretvaranje u izvorni oblik

Pri radu s binarnim vrijednostima prikaz u heksadekadskoj bazi često je prikladniji i jednostavniji jer su vrijednosti čitljivije ljudskom oku. Pretvaranje u heksadekadske vrijednosti u CyberChefu radi se opcijama „to/from Hex“. Dobivene vrijednosti moguće je odijeliti željenim znakom (*delimiterom*): razmakom, zarezom (prikazano na slici), točka-zarezom, itd. Pri vraćanju u početni oblik moguće je odabrati određeni *delimiter* ili automatskim načinom omogućiti automatsko prepoznavanje koje se uglavnom uspješno izvrši.



Slika 5. Pretvaranje u heksadekadske vrijednosti odijeljene zarezom

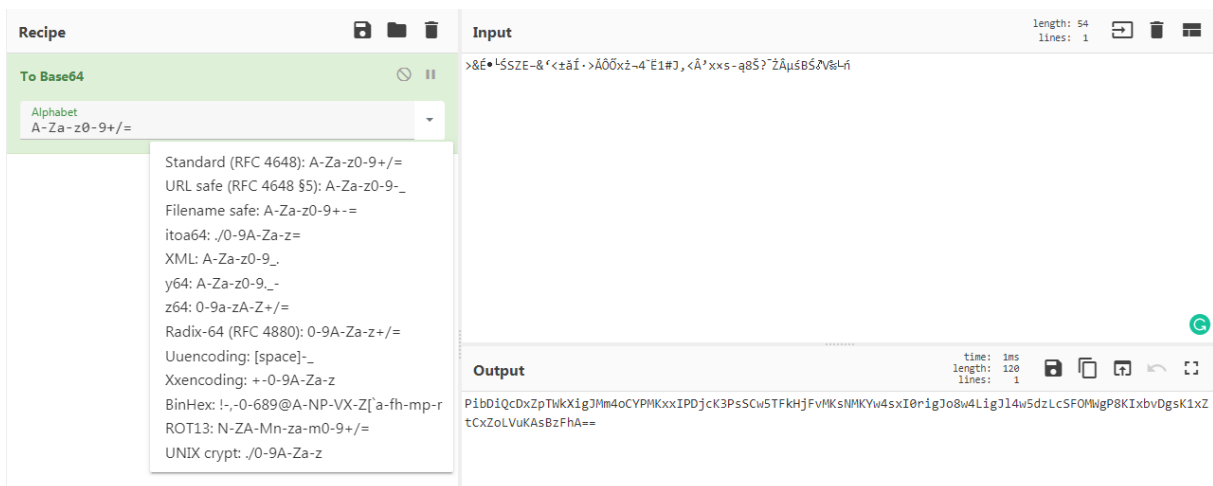


Slika 6. Pretvaranje u izvorni oblik s automatskim prepoznavanjem delimitera

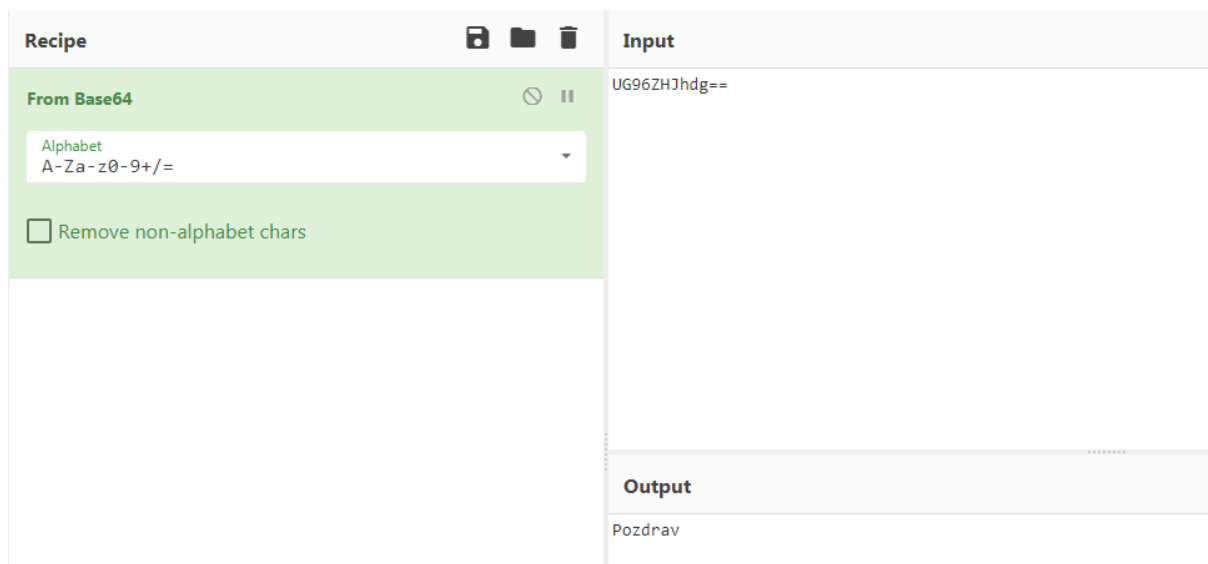
3.2 Base64

Base64 kodiranje pridonosi što sigurnijem prijenosu podataka između različitih sustava, bez da se poslani podaci izmijene u tom procesu. To se ostvaruje tako da su u izlaznim podacima (Base64) dozvoljeni „jednostavni“ znakovi: samo brojke, slova engleske abecede i par simbola. Postoje različite varijante koje je moguće odabrati.

U ovom alatu ovakvom kodiranju i dekodiranju služe opcije „to/from Base64“.



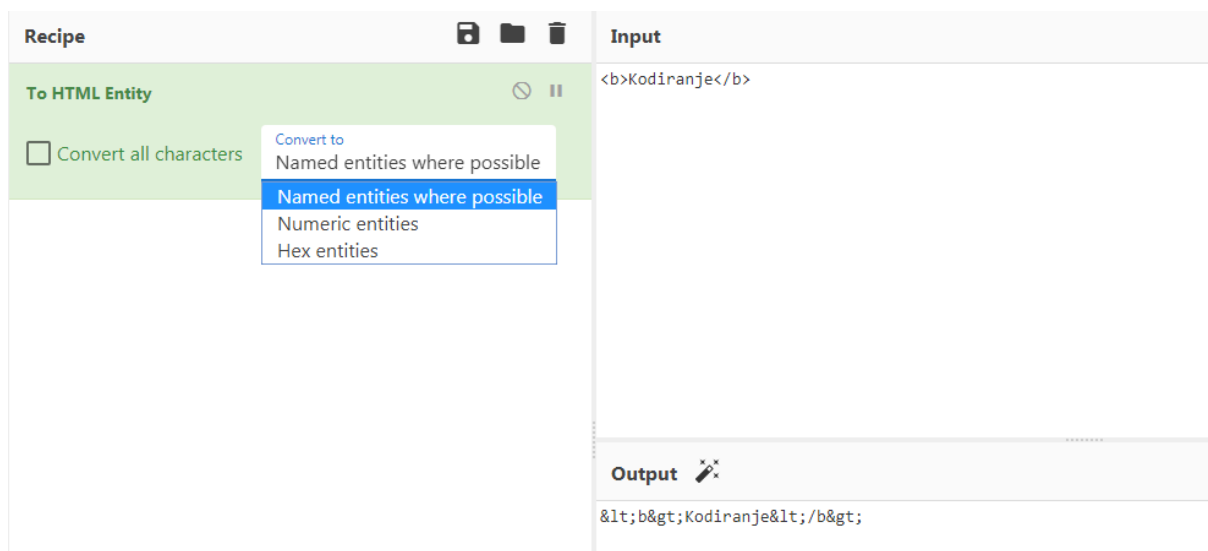
Slika 7. Base64 kodiranje



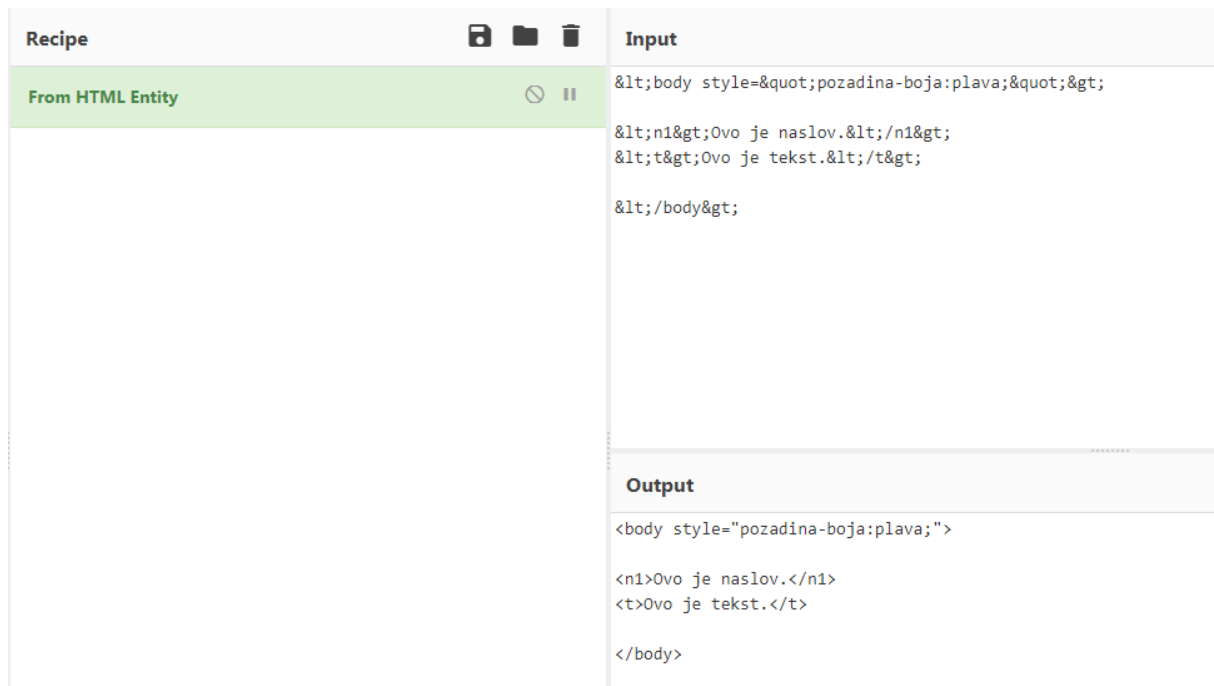
Slika 8. Base64 dekodiranje

3.3 HTML

HTML je jezik za izradu i vizualno oblikovanje web stranica. Opcija „to HTML Entity“ će znakove koji imaju posebnu svrhu i značenje u HTML-u kodirati u drukčiju oznaku. Ponudeno je i više vrsta *entityja*: numerički, heksadekadski i imenovani. Dekodiranje je moguće uz opciju „from HTML Entity“.



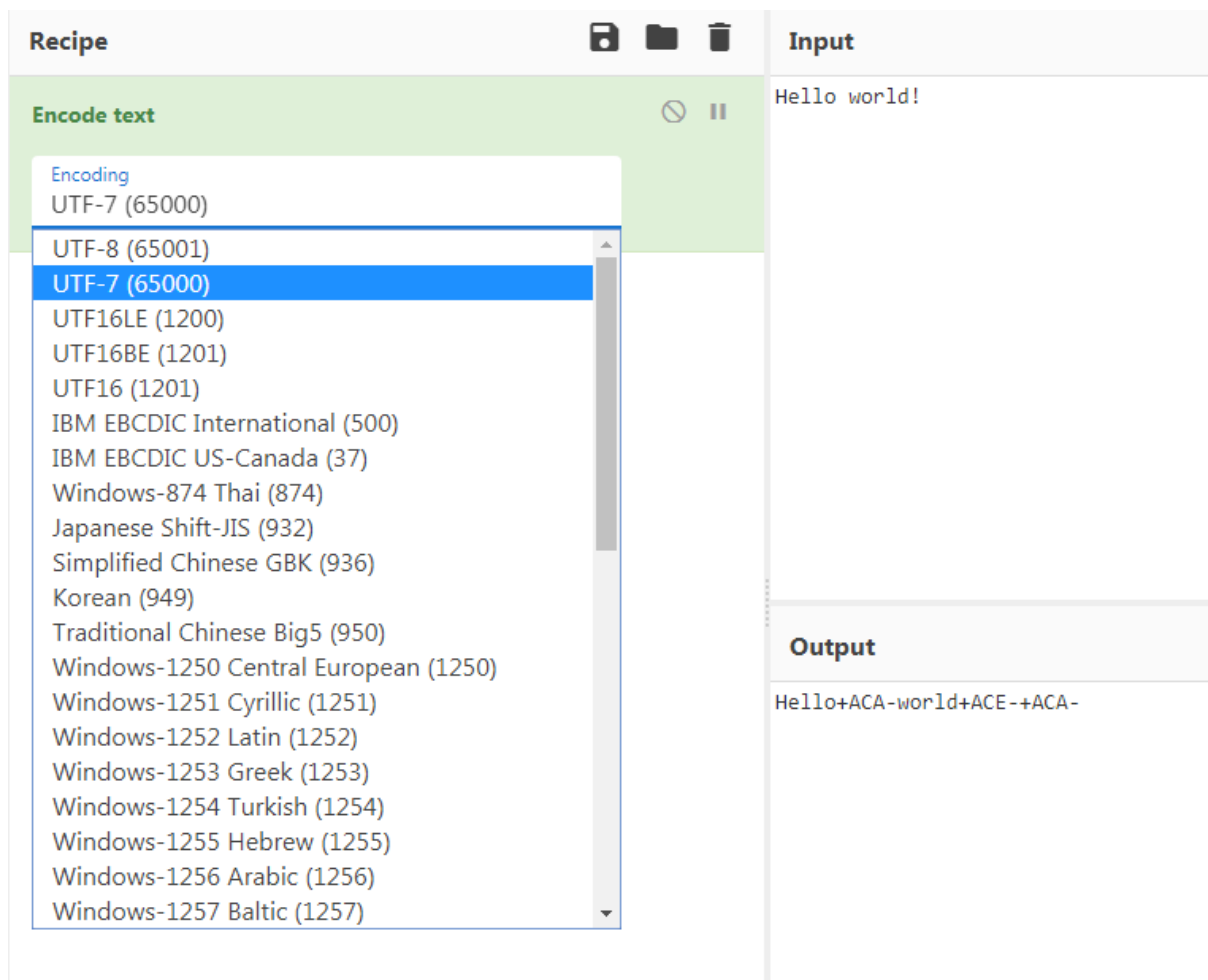
Slika 9. HTML Entity pretvorba



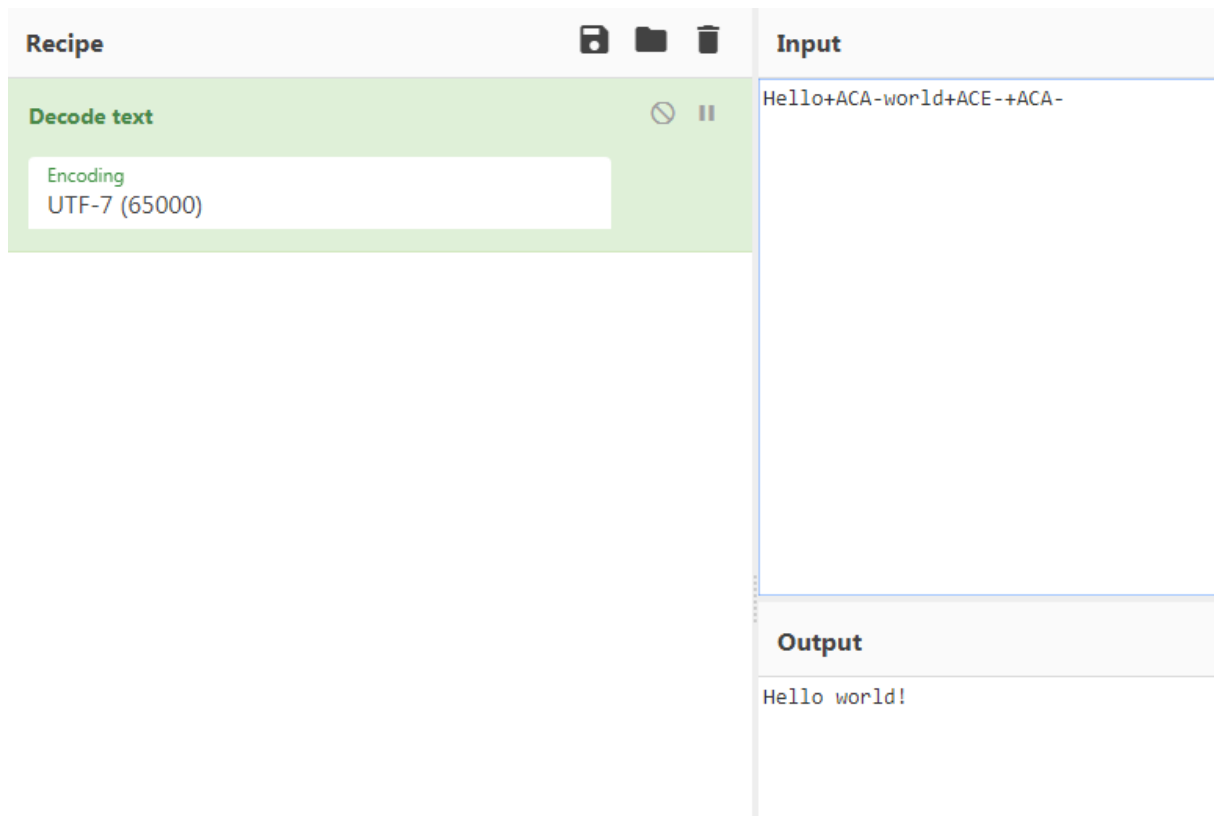
Slika 10. Pretvorba u izvorni oblik

3.4 Kodiranje znakova

Kodiranjem teksta niz znakova prikazuje se na specifičan način određen nekim kodnim sustavom. Ono se primjenjuje u računarstvu, pohrani i prijenosu podataka. Funkcija „Encode/Decode text“ omogućuje kodiranje i dekodiranje teksta na različite načine koje korisnik može izabrati (kao što je prikazano na slici 11), npr. UTF-7, UTF-8, UTF16, ISO-8859-1 do ISO-8859-16, itd.



Slika 11. Kodiranje UTF-7(65000)



Slika 12. UTF-7 dekodiranje

3.5 JSON

Alat „CSV to JSON/JSON to CSV“ je koristan kada postoje neki JSON podaci koje je npr. vratio API web stranice, a želimo ga prebaciti u CSV koji se onda može lako pregledavati i uređivati u Microsoft Excelu/LibreOffice Calcu i sličnim alatima, kao što je vidljivo na slici 13.

Recipe
📁 🗑️
Input

CSV to JSON
🔍 ||

Cell delimiters
,

Row delimiters
\\r\\n

Format
Array of dictionaries

Output

```

[
  {
    "Godina": "1997",
    "Proizvođač": "Ford",
    "Model": "E350",
    "cijena": "3000.00"
  },
  {
    "Godina": "1999",
    "Proizvođač": "Chevy",
    "Model": "",
    "cijena": "4900.00"
  }
]

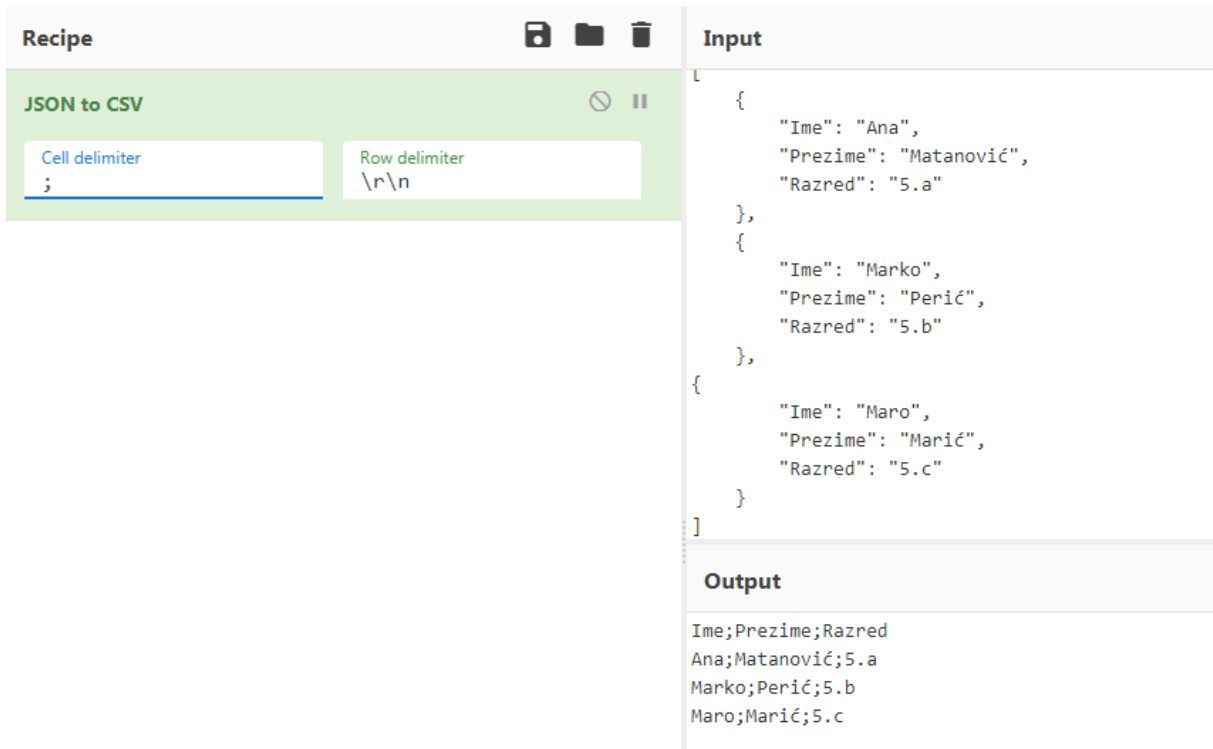
```

STEP

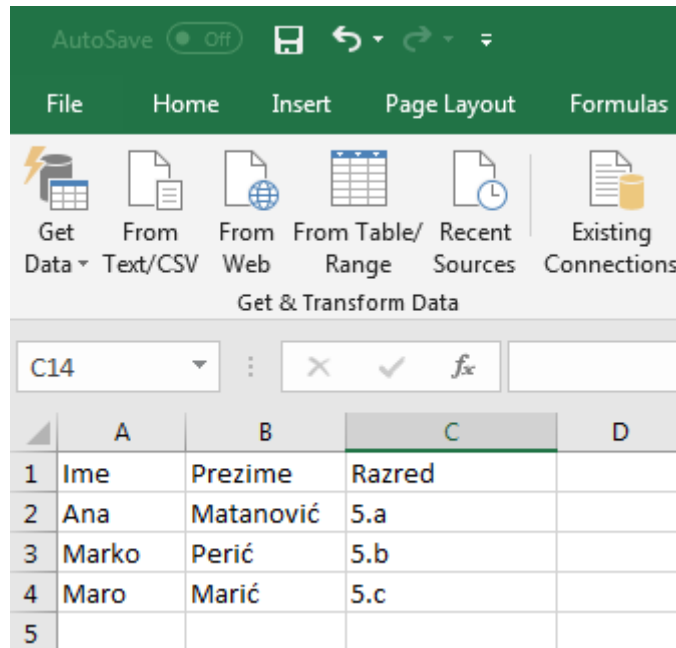
👨‍🍳
BAKE!

Auto Bake

Slika 13. Pretvorba CSV formata u JSON oblik



Slika 14. Pretvorba iz JSON-a u CSV format

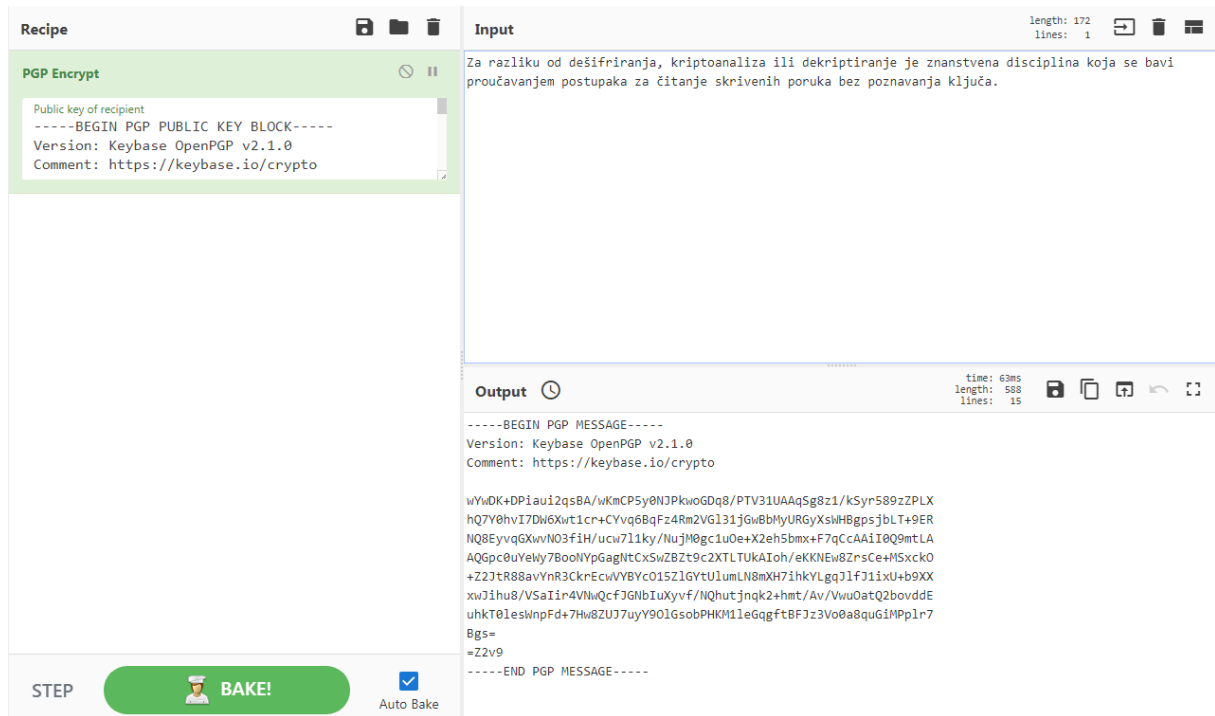


Slika 15. CSV podaci prebačeni u Excel

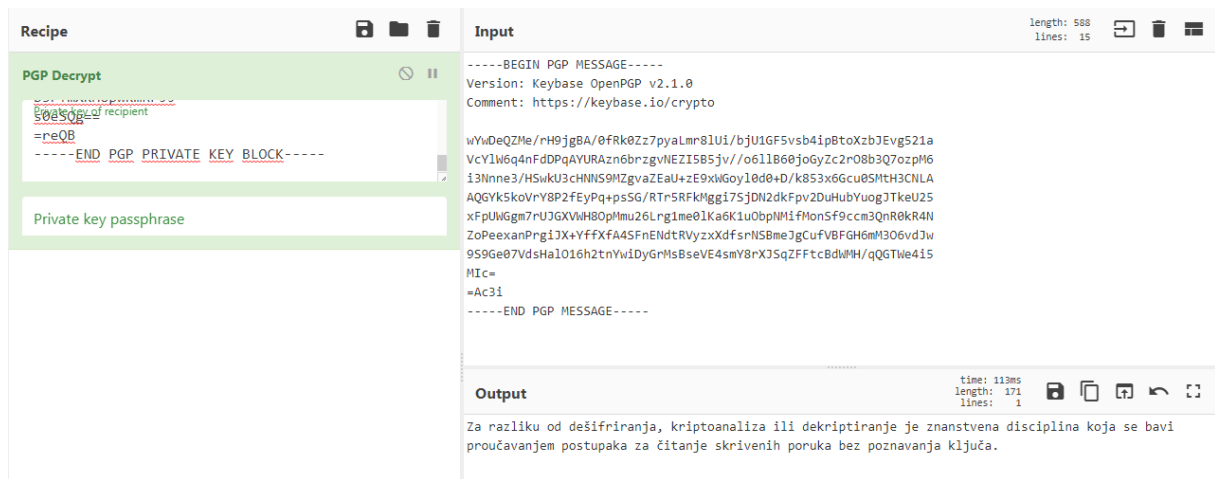
3.6 PGP

Sljedeći korisni alat koji nudi aplikacija je „PGP Encrypt/Decrypt“. PGP (engl. *Pretty Good Privacy*) je standard za kriptiranje, dekriptiranje i potpisivanje poruka koji korištenjem privatnog i javnog ključa omogućava sigurniju komunikaciju. Za kriptiranje poruke služi javni, a za dekriptiranje privatni ključ. Oni su povezani složenim matematičkim

funkcijama i gotovo je nemoguće otkriti privatni ključ preko javnoga, čime se osigurava da poruku može pročitati samo vlasnik privatnog ključa.



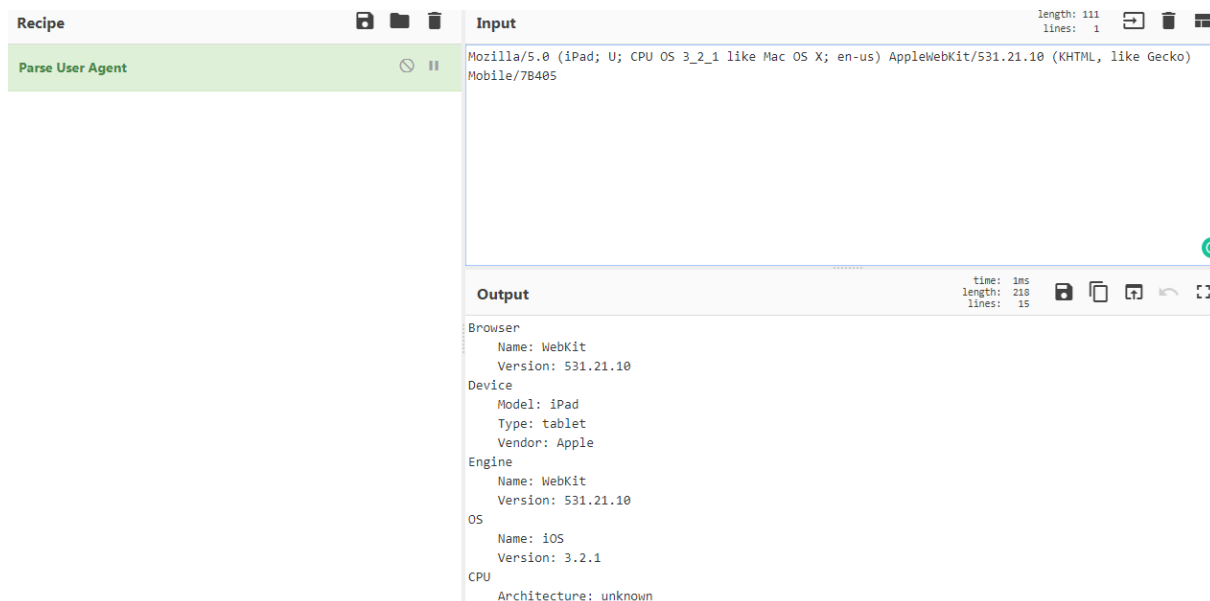
Slika 16. PGP kriptiranje poruke



Slika 17. PGP dekriptiranje poruke

3.7 Parse User Agent

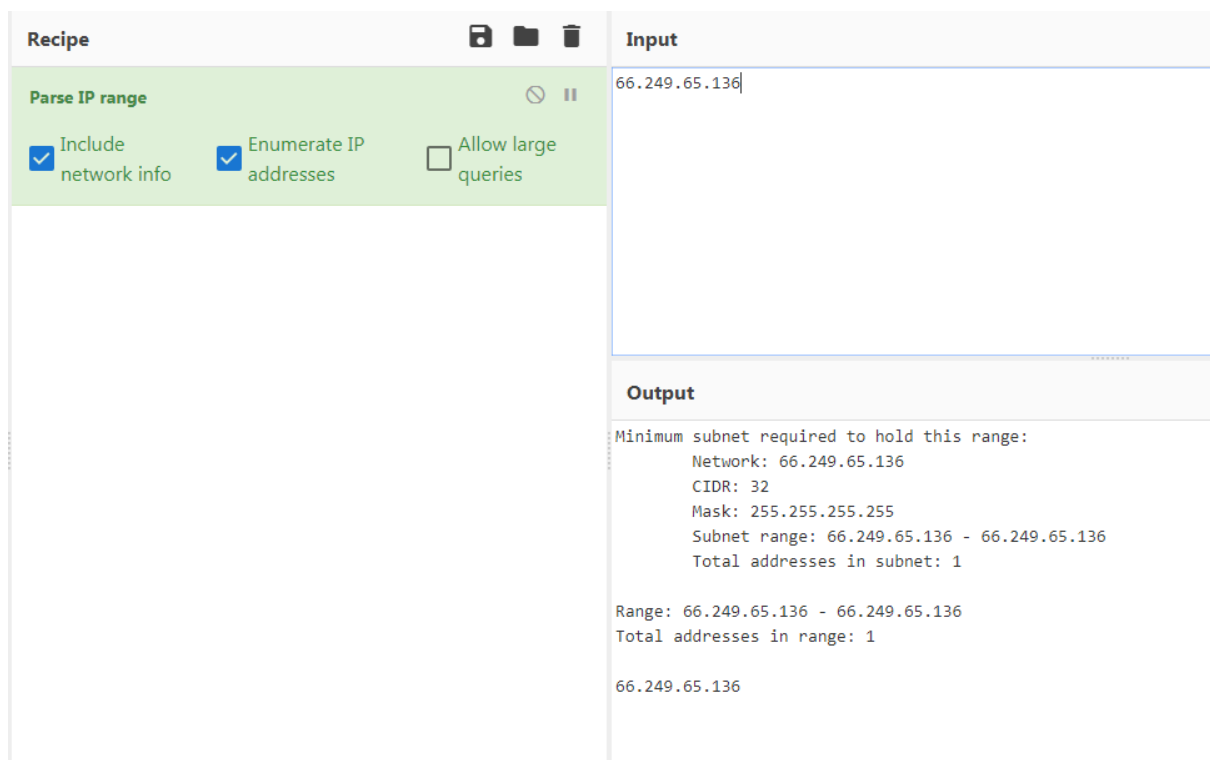
Alatom „Parse User Agent“ radi se identifikacija i kategorizacija sadržana u *user agent* podatku koji se unese. „User agent“ je jedno od uobičajenih zaglavlja u protokolu HTTP koji se koristi za pregledavanje weba. Podatak sadržan u tom zaglavlju daje informaciju o imenu i inačici web preglednika, operacijskog sustava i slično.



Slika 18. Parse User Agent

3.8 Parse IP range

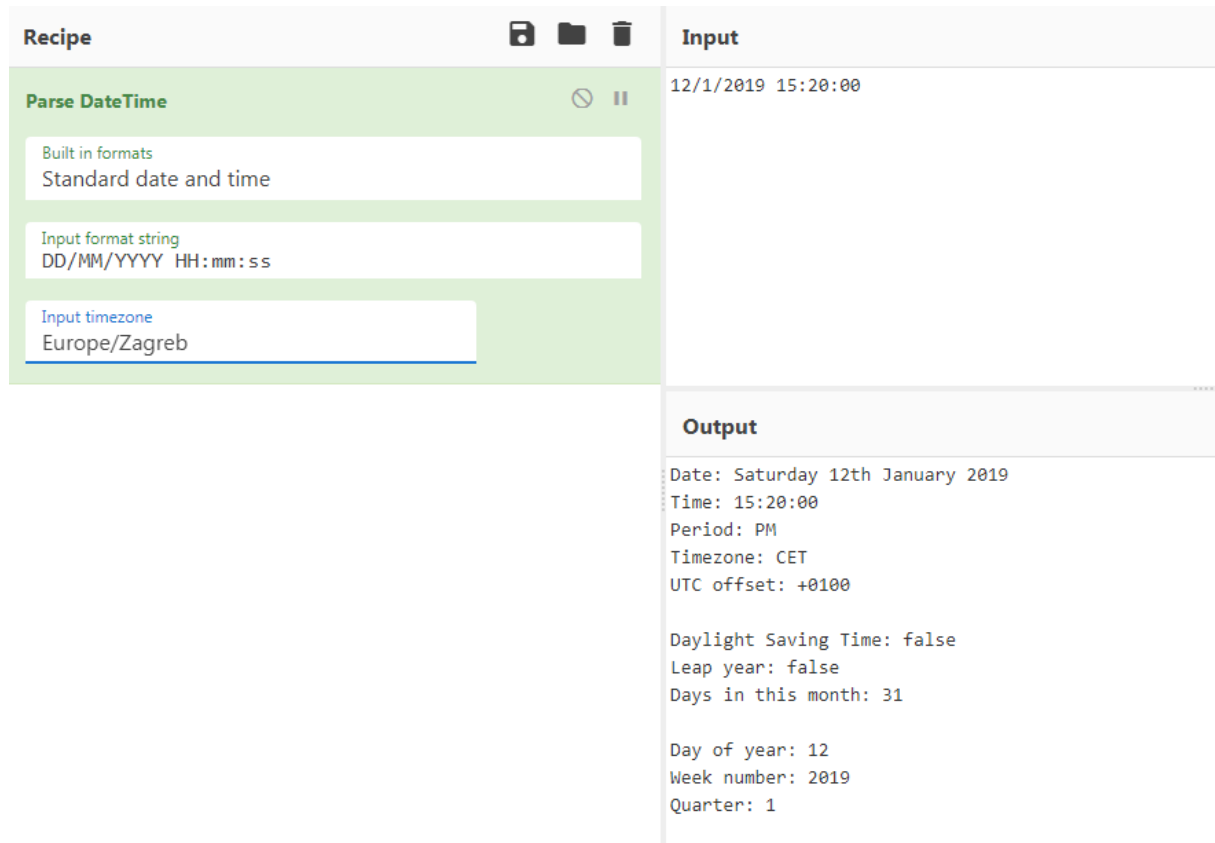
„Parse IP range“ za neku IP adresu odnosno za raspon IP adresa prikazuje mrežne informacije.



Slika 19. Parse IP range

3.9 Parse DateTime

Alatom „Parse DateTime“ uz unos vremena i datuma, čiji format je moguće odabrati po želji, ispisuju se dodatni podaci kao što su dan u tjednu, je li godina prijestupna, ukupan broj dana u tom mjesecu, i dr.



The screenshot shows the 'Parse DateTime' tool interface. The 'Input' field contains the string '12/1/2019 15:20:00'. The 'Output' field displays the following information:

```
Date: Saturday 12th January 2019
Time: 15:20:00
Period: PM
Timezone: CET
UTC offset: +0100

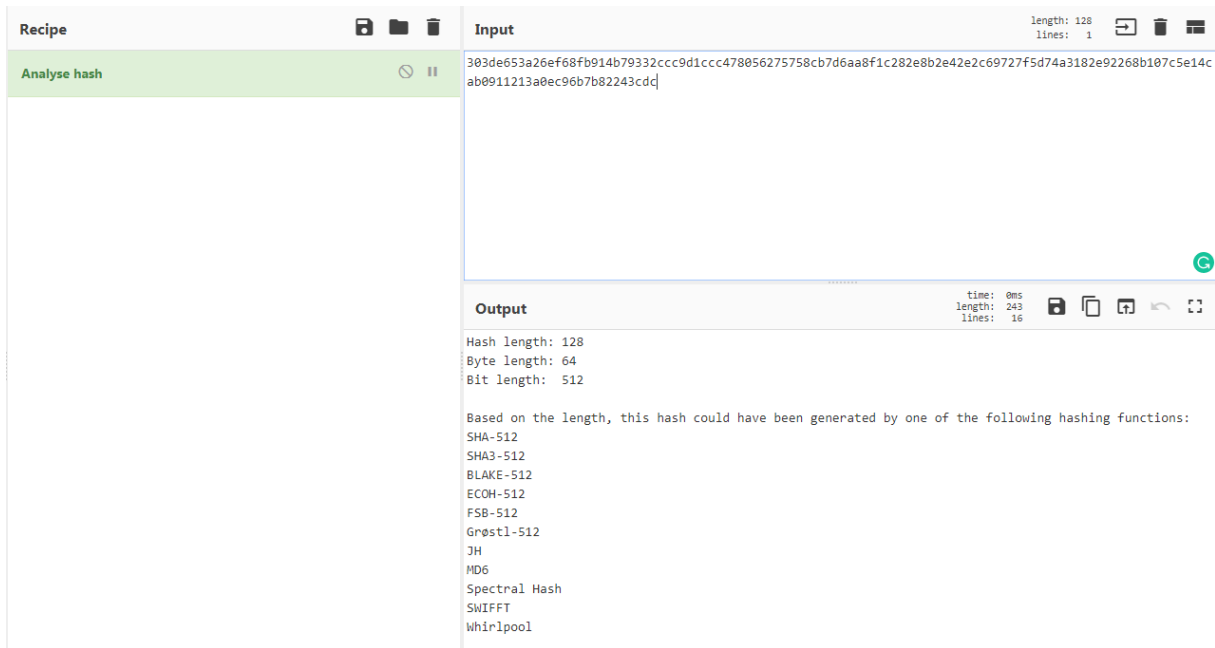
Daylight Saving Time: false
Leap year: false
Days in this month: 31

Day of year: 12
Week number: 2019
Quarter: 1
```

Slika 20. Parse DateTime

3.10 Analyse hash

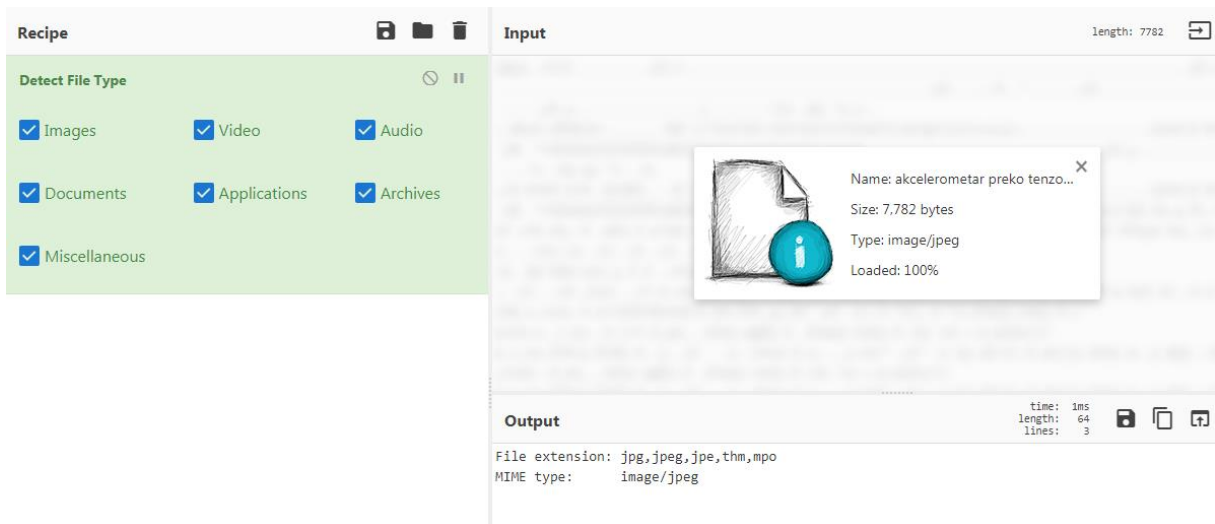
Kriptografske funkcije sažetka (engl. *cryptographic hash functions*) imaju puno primjena. Primjerice, one se koriste kod provjeravanja integriteta datoteka, tvorbe digitalnih potpisa te kod sigurne pohrane lozinki. Opcija „Analyse hash“ u „Cyberchefu“ analizira heksadekadski izlaz kriptografske funkcije sažetka kako bi pomogla u određivanju algoritma sažetka koji je korišten.



Slika 21. Detekcija hash funkcije korištene u poruci

3.11 Detect File Type

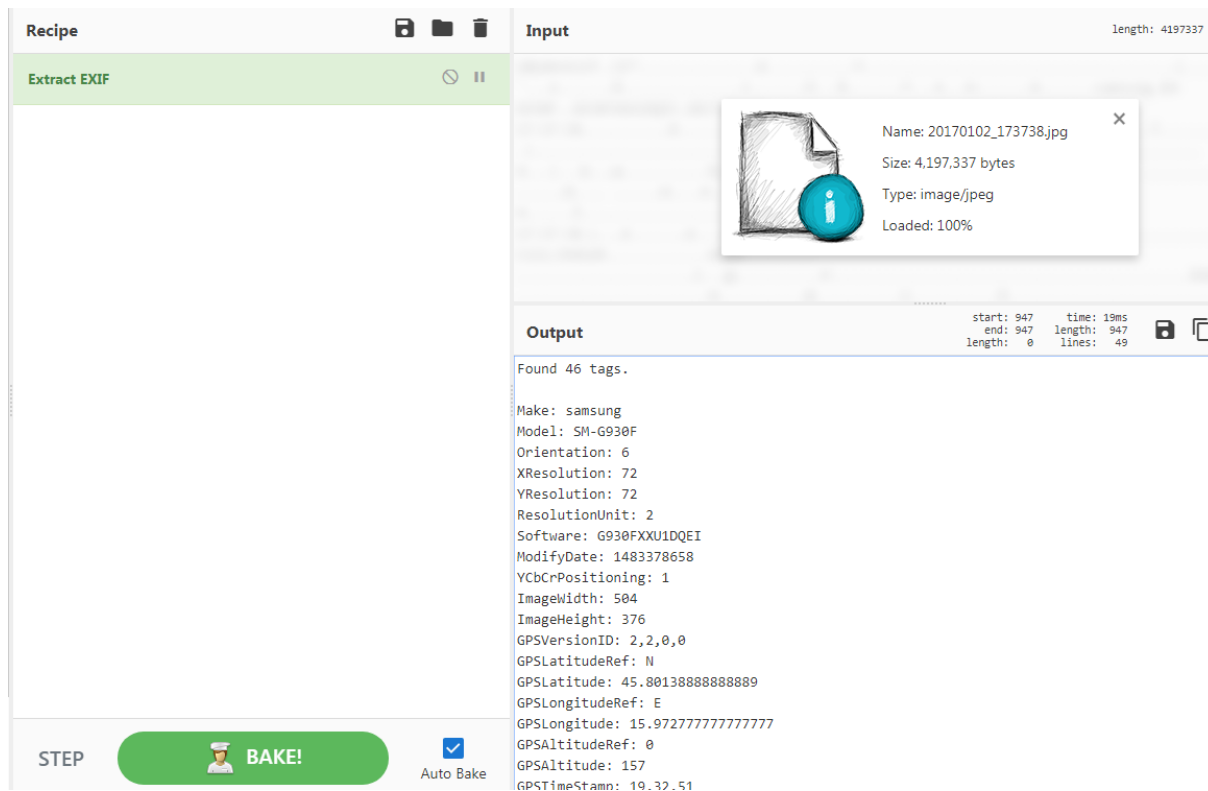
Nudi se i mogućnost otkrivanja vrste datoteke: uz opciju „Detect File Type“ alat prepoznaje radi li se o slici, videu, zvukovnom zapisu ili nekom drugom datotečnom tipu. Na slici 22 prikazana je detekcija slike.



Slika 22. Prepoznavanje slike

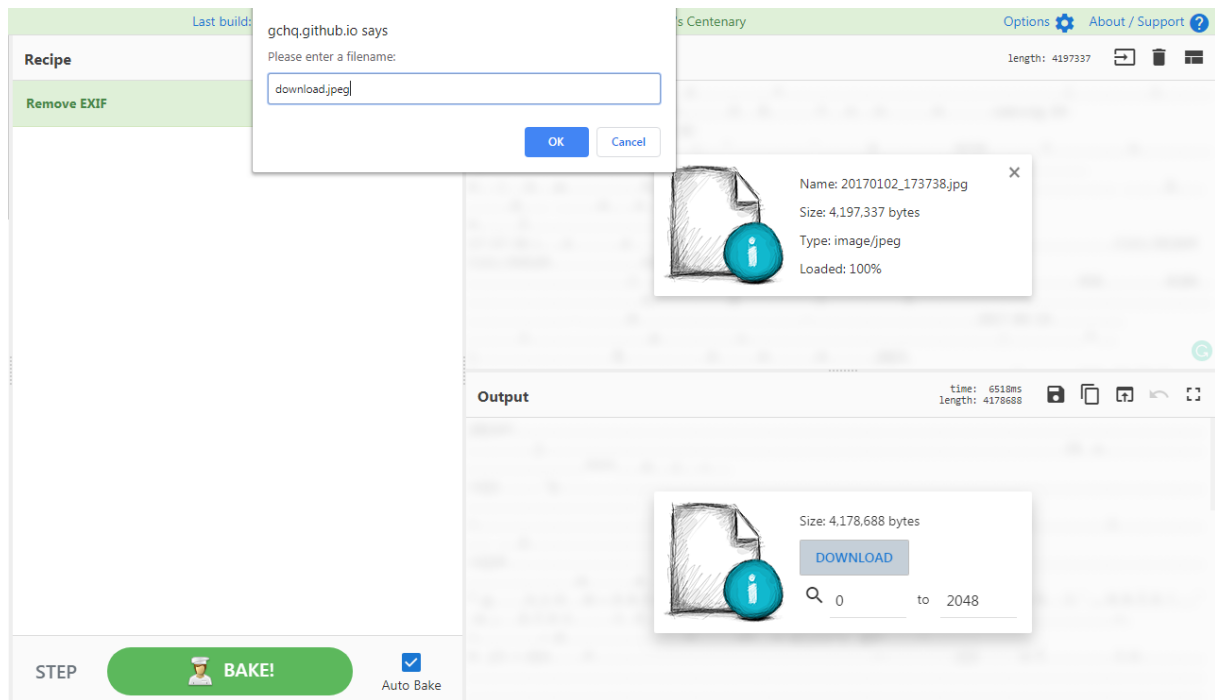
3.12 EXIF

EXIF podaci iz slikovnih i zvukovnih datoteka sadržavaju informacije o samoj datoteci i uređaju kojim je snimljena. Alat „Extract EXIF“ ispisuje te podatke iz zadane datoteke, kao što je prikazano na slici 23.



Slika 23. Opcija Extract EXIF

Komplementarnim alatom „Remove EXIF“ može se kreirati i preuzeti kopija datoteke koja neće sadržavati spomenute podatke.



Slika 24. Opcija Remove EXIF i preuzimanje nove datoteke

4 Zaključak

Alat „CyberChef“ koristan je za sve koji se bave obradom i analizom digitalnih podataka, pa čak i one bez matematičkih znanja potrebnih za samostalno pretvaranje podataka u željeni format. Nudi širok izbor alata za obradu podataka: od različitih kodiranja, kriptiranja, aritmetičkih i logičkih operacija, do prepoznavanja i obrade multimedijjskih datoteka.

Jednostavno i intuitivno sučelje aplikacije, bazirano na *drag and drop* funkcionalnosti, te mnoge korisne opcije omogućavaju lako i brzo snalaženje u programu.

Moguć je *online* pristup alatu na [web stranici](#) ili *offline* pristup uz preuzimanje aplikacije na vlastito računalo, čime je osigurana privatnost korištenih podataka, bez njihova slanja na vanjsku stranicu.