

# STEGANOGRAPHY

GOVERNMENT DOCUMENTS UNDER ANALYSIS

COMPROMISED DEVICES  
VULNERABLE SOFTWARE

BLACK SEO  
SECRETS  
MESSAGES

Content created by  
Alexandru Angheluş

[www.prodefence.ro](http://www.prodefence.ro) | [contact@prodefence.ro](mailto:contact@prodefence.ro)

**Steganography** (/ˌstɛɡəˈnɒɡrəfi/ (listen) STEG-ə-NOG-rə-fee) is the practice of concealing a message within another message or a physical object. In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video. The word steganography comes from Greek steganographia, which combines the words steganós (στεγανός), meaning "covered or concealed", and -graphia (γραφή) meaning "writing - Wikipedia

## STEGANOGRAPHY

TEXT

IMAGE

AUDIO

PROTOCOL

DOCUMENTS



2012

**DECLARAȚIE DE AVERE - rectificativă**

Subsemnatul \_\_\_\_\_, având funcția de \_\_\_\_\_  
la AGENTIA NAȚIONALĂ \_\_\_\_\_  
CNP. \_\_\_\_\_  
domiciliul la \_\_\_\_\_

2019

**DECLARAȚIE DE AVERE**

Subsemnatul/Subsemnata \_\_\_\_\_, având funcția  
la Agenția Națională \_\_\_\_\_  
de \_\_\_\_\_  
CNP \_\_\_\_\_ domiciliul Jud. \_\_\_\_\_

NR. 2020

**DECLARAȚIE DE AVERE**

Subsemnata \_\_\_\_\_, având funcția  
de \_\_\_\_\_ la Agenția Națională \_\_\_\_\_  
CNP \_\_\_\_\_ domiciliul \_\_\_\_\_

cunoscând prevederile art. 292 din Codul penal privind falsul în declarații, declar pe proprie răspundere că împreună  
cu familia<sup>1)</sup> de la  
următoarele:

What you see is a proof of three government institution documents hosted on the official servers.  
Important aspects:

- Three different people
- Three different years
- The same institution (National Agency...)

If you haven't noticed anything special in these images it's normal. During this analysis you'll notice some details that make the difference and will make you wonder about some things.

These questions appear are covered on this analysis.

NR. [redacted] 2020

## DECLARAȚIE DE AVERE

Subsemnatul/ Subsemnata [redacted], având funcția

de [redacted] la Agenția Națională [redacted]

CNP [redacted], domiciliul [redacted]

conștient de prevederile art. 292 din Codul penal privind falsul în declarații, declar pe propria răspundere că înțeleg și  
cu familia<sup>1)</sup> de la  
următoarele:

Subsemnatul/ Subsemnata [redacted], având funcția

de [redacted] la Agenția Națională [redacted]

CNP [redacted], domiciliul [redacted]

Subsemnatul/ Subsemnata [redacted]

[redacted]

Subsemnatul/Subsemnata, \_\_\_\_\_

de \_\_\_\_\_ la \_\_\_\_\_

CNP \_\_\_\_\_, domiciliul \_\_\_\_\_

Correct! The lines of the form are neither continuous, nor dotted, nor curved. They contain multiple of meaningless characters and look like the words in the form (you can't notice the difference between the rest words).

Let's leave it for now. The difference between an original but unscanned form and a completed and scanned form is clear.

The clarity is significant, but the document scanned and used by the Institution raises questions.

When creating a document in Word there is the option to insert tables and change the styling. One of them is cell border styling, having to choose from a predefined list.

Taking into account what we have already shown, it can be seen that the lines of the table are visibly modified, including some characters that are difficult to read (for now).

**NOTĂ:**  
Se vor declara inclusiv cele aflate în alte țări.

Adresa sau zona	Categoria*	Anul dobândirii	Suprafața	Cota-parte	Modul de dobândire	Titularul <sup>2)</sup>

**NOTĂ:**  
Se vor declara inclusiv cele aflate în alte țări.

Adresa sau zona	Categoria*	Anul dobândirii	Suprafața	Cota-parte	Modul de dobândire	Titularul <sup>2)</sup>



The first three examples are good for further analysis and to identify the characters included in the document.







Let's ask Google for some help |  
webcache.googleusercontent.com/search?q=cache: + document

Analyzing the html version of the online document

```
urderisce caSENEGALE H f aø set asked Hacked lead 'mall (mind al media madalam mel me dedi |-----AZER ZAPALAZARATING MANISPANJANKA ddad kuodukanda
SPİTALINLANLEKT STEAMTLINE ISLAND
PERTVANSERSI PASANTA IN ANNAN
===\ATTREPRISEN LISAPRASPLESALE di 'dhd amould kom mlamak powder thumpdaydik pop=- - - - podoppi
STTTTIMASSAGE TAVAPILNdte al 'n hou die Talk Time man die stam de ala ala kommu'a amada amaldammadla mammamda mama ya-----
-----IT 19ATATI PRIJSW aø Hal Valeado 8 8. Pakel la ada ada al 'lalu ada ada ada alumnanda ada alumn-----ETDIYYNNI
|-----|--AVESTE NEPREM 1950 1 ade keldle Makeun ka' dan 'kong kaka a kommeden mmm de um pro ampak op ) -- |--| ---- {AMPILAN LAMA PLATJANAKun kmalukukud podem adsde
TOILETROTTSLAZE LEPANTERWYZWA LAMPAATIA JA KATKA K 1 de dak ko lahko dodaeth aman die dankie aande di alamanda da je dodao da dan mena alam que alumnas dienas die
-TİMAN AWITTEETTIAM ELIT IN LEVITAE LINGIMUVINA de l' al l dl ka nan pla madena dle ale mama anda ada malagkap på mo ma
¶'-----LUTEEMAN MELAWA amar man kund www.warm-maal kukka kukabido al alanda e ade all al Palauall anda de rodead a dat lokal baka ada pela
www.my/ -----ý dili kum kumə-y----- MARDKA Pod kk kulkkik ma ka ma ka ma ka ma-
mpanyinginya. (*/**1/21/2" Pilkada Jalad ay m-----17-115--11--1/SENYAMPA La Val Tim' makali nisu u de de la Banda ng kopol akyakan almapla
mannen met de monument manalo ada a mena de mie man skade spelade pokey==myakimya-TEMTW/MITH SETTE AMAVARAMETELLAAN ANALALAMAN AMELLAPOTATITANIA MALAPMADAWATI LANAN
ITINTTWIKISAN KAPPA K Mala ka atkal atat a la mitad desdeskunde mil aø skemmdes valestinal penemu valencleum-p=====SA) 1990 ANAITAY 2165 SƏNƏLMAM PYLPAIKAMPPAI
Tillmm ka mmoja de umm y mldən nəm 112 lSTEPHEDEN WEWENAAN DENGAN JARUM PENANAMAN d' c d ma di oily dan di dan mmm mm kg pa -----EPTAMANNAKAKAPAN JIKAMARI
```

Good thing that a phrase in the  
first line containing the word  
“HACK” appeared, otherwise  
I'd feel like I was working in  
vain.



It seems that we cannot find any meaning in the  
word sequences, if we were supposed to find one or  
if the document was intentionally modified.

Do you have the courage to continue the analysis?



I'm glad you have the courage! The analysis is now starting to get very interesting!

Extracting the text from those small portions of the document did not help much, but it did provide some clues for further exploration of the secrets and hidden messages.

I chose to extract the Arabic characters from the whole document page by page.  
Sometimes the writings can only be understood as a whole and not just in parts individually.  
If there is a message there, the whole thing should be visible.  
And of course, let's not forget that the characters in the document also seem modified.

The following led me to analyze not just one document, as I initially established, but all three documents discovered.

[www.prodefence.ro](http://www.prodefence.ro) | [contact@prodefence.ro](mailto:contact@prodefence.ro)

*Rotao and the cities of Imarwa, Waz, Lamyā, Azrasa, and Azmbamzeh, Moatazzam, Aazgermar, and Ramak Zab."*

7 \* 0 5 7  
What do you eat

Amaak Saw, Rama, Mamsij Al-Sarm, Awa, Rat Loh, and #Tedmma, Mmm,  
Kaolinar 1["wa2"]  
And Al-Ajmtat / Bara'un, but the uncle

I love you  
6 #uncleo0  
Moh grom, flopprime grorum, "Wellstamiyama, I, and I, Ajroa with a stick, and  
"Arana" / 77" (\*2)

And for Masij that a common thief Ra'ao survived Jim 1 "Wal: A stinger of a maha duck's sting, by Marv, and Tizmat/Abnzem, Antafara 11)  
Core of luxury

11 It is important for people, it is put, and it is a piece of diamonds for the  
stomach, it is not allowed to eat, it is like a lump in it.  
liv tatón pain i'm sartal  
the water

**[www.prodefence.ro](http://www.prodefence.ro) | [contact@prodefence.ro](mailto:contact@prodefence.ro)**

# Yesser Saber

Al Mitla Baalik 1 on the list, gear 001, hint

*Maaysi Ba for your goodness*

*A few features that are for his visitors, the most embarrassing, from the conjunctiva, the defect of the determination of Ab Sama Raya (/\*)*

O, on the authority of Ibn Mazjarin Alaiya, "Miradine Makhwa Darl A Zar

0 041 0 20110 May Tra. Prague

Don't worry about me: 0 0.:

The worms are shy

1 A.D. 11 (in Belmedsan Rum, the king of Sarurir. Al-Bajruitir from / A. Beitoui, Z.

Al-Ambar, and Ba'ram, mm Mayra) “Ba (2?\*)

Wamim bin Wim Aw Luo Ullamiya Al-Af 0 m to Al-Sayyut Amard

*I took a moment to swallow the poison of Absaline He was healed ©1) Ragal*

*Ola bin Abivazir is familiar with the titles of Bejjoul, Buza Sala*

Give birth 00 2010: 2

*Burt Tabert threw the lone ring or two on 000.*

To increase the prayer, my voice is narrowing down on #Mmsatasta, what?

Attiila Darsi Arirag, to say: "Jetima Masa'iji 1 will be left in pain

*You will listen to me, as you wish, to come to the best of light, to tell the story of a group of people with whom we slander our country, yelling together at the right time.*

*Yes, there are 3,000 products, and they have been tamed by Tamoaz Basa'i with his glance.*





**ProDefence**  
Cyber Security Services

Do you understand now why I wanted to continue this analysis?

- The truth is that what is presented here is a part of only 15% of the whole analysis.
- Almost 25 hours spent on this analysis finally gave this interesting result.
- The truth is that the results of the texts are longer, but I've chosen what I found most interesting in order to create this report.

Initially, I thought that the documents were modified in order to create traffic for certain keywords in search results. Black SEO consists of various illegal methods, and using online documents is one of those.

From what is observed, they seem to be excerpts from different discussions, on different topics and a content full of names of people and geographical regions. So we can frame everything in SECRETS and MESSAGES.

BLACK SEO  
SECRETS  
MESSAGES

I can tell you for sure that I do not know what these documents represent or what their ultimate purpose is. 100% of these government documents have been modified by someone, a threat actor or a system.

However, their existence raises questions from a cyber security perspective.

For now, I can only imagine a few ways in which the documents have reached this state.

- The computer used to edit them is compromised.
- The software used is modified to insert those characters into documents.
- The server of the Government Institution is compromised and someone has made the necessary changes.

The need to secure the entire infrastructure is critical.

Digitization started off on the wrong foot. Education should have been placed first before anything else. There is only a tiny number of specialists who work in government institutions.

If this seems random or of low severity ... think about what I mentioned earlier (server, computer, software) and the implications of each element's personal and confidential data that may be compromised and exploited by cyber criminals.

Cyber security is more than just an update and an SSL certificate





MORE THAN CYBER SECURITY  
PASSION

Content created by  
Alexandru Angheluş

[www.prodefence.ro](http://www.prodefence.ro) | [contact@prodefence.ro](mailto:contact@prodefence.ro)

