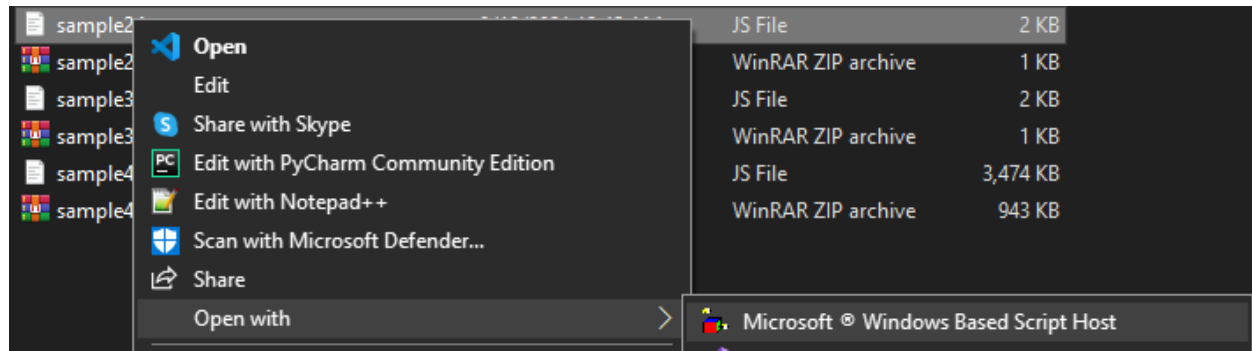


Mîndruleanu Matei Daniel - tema 5 SSI

### Exercitiul 1:

Am încercat să rulez scriptul cu Microsoft Windows Based Script Host și am obținut următoarele rezultate:



Windows Script Host



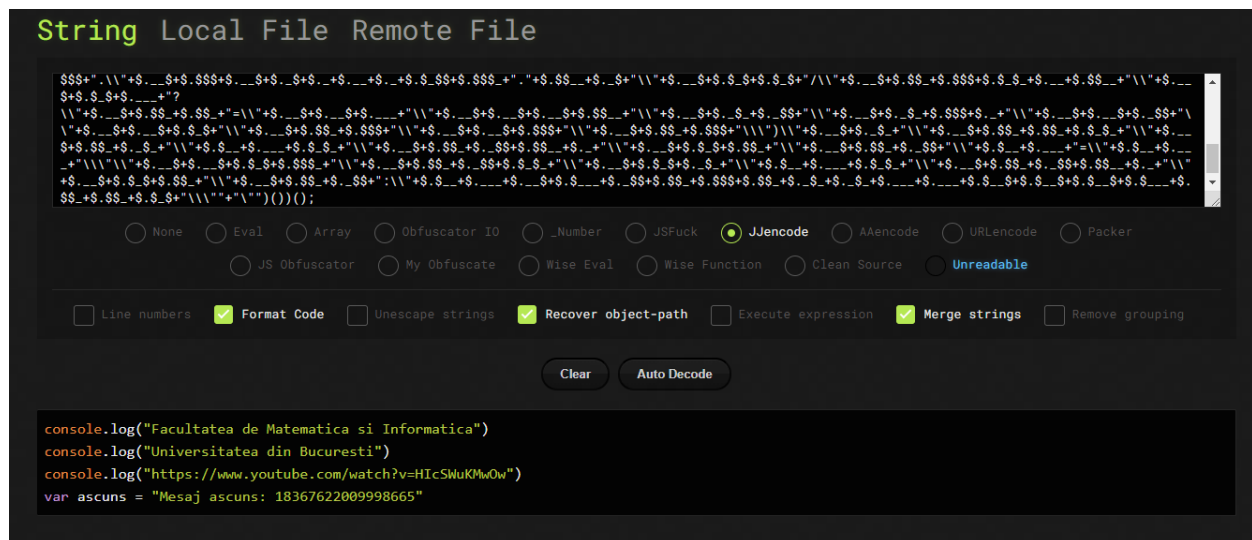
Script: C:\Users\Matei\Desktop\UNI\Anul III\SSI\lab\samples\sample1.js  
Line: 1  
Char: 409  
Error: '\$,\_\_\_[...]' is null or not an object  
Code: 800A138F  
Source: Microsoft JScript runtime error

OK

Am rulat codul din arhiva de la primul sample în Visual Studio Code și am aflat că acesta afișează în consolă

```
[Running] node "c:\Users\Matei\Desktop\UNI\Anul III\SSI\lab\samples\sample1.js"
Facultatea de Matematica și Informatică
Universitatea din București
https://www.youtube.com/watch?v=HIcSWuKMwOw
,link-ul fiind "rickroll, but it never starts 10 HOURS" de pe YouTube.
```

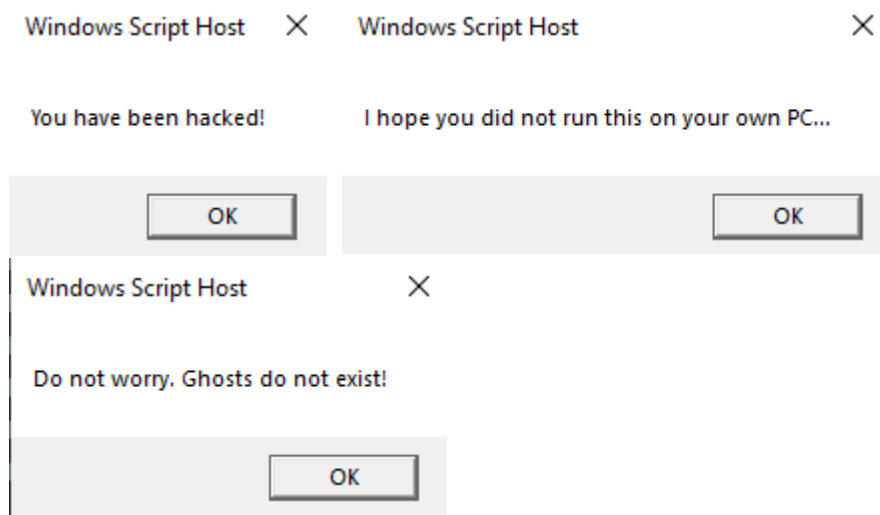




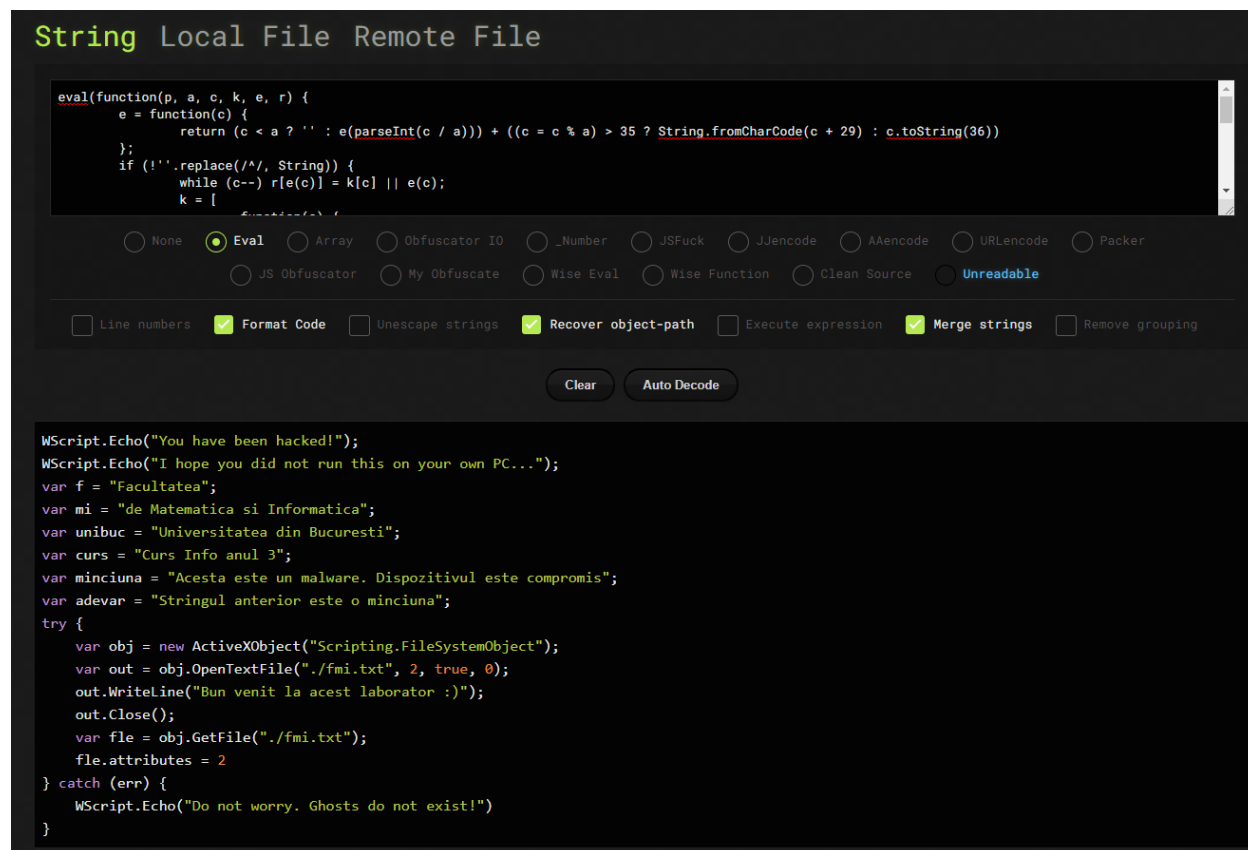
Codul a fost scris de o persoana care a vrut ca cei la care ajunge acesta sa nu il poata descifra.

## Exercitiul 2:

Am incercat sa rulez scriptul cu Microsoft Windows Based Script Host si am obtinut urmatoarele rezultate:



Rularea codului in visual studio code nu s-a putut realiza, asa ca am trecut la analizarea codului direct in <https://lelinhtinh.github.io/de4js/> folosind Eval pentru urmatoarele rezultate:



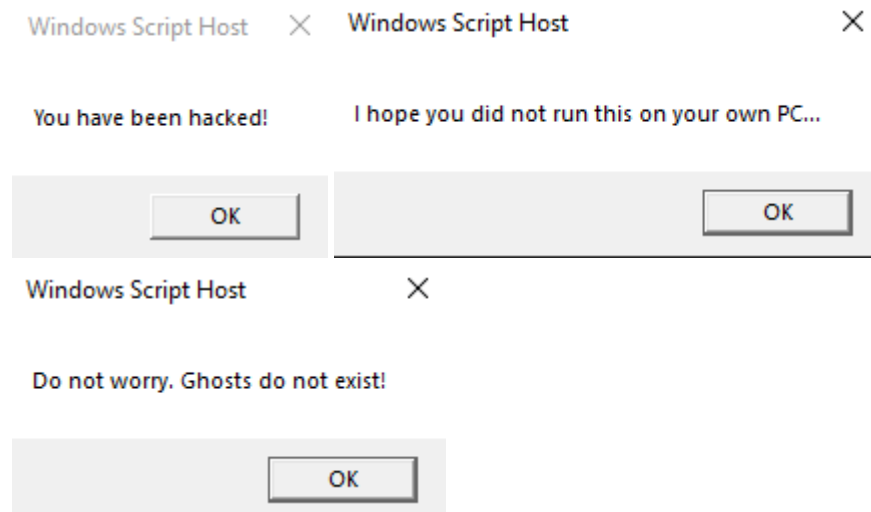
Codul afiseaza mesajele: "You have been hacked!" si "I hope you did not run this on your own PC..."

Dupa care incearca sa creeze fisierul fmi.txt in care sa scrie "Bun venit la acest laborator", dar daca prinde vreo eroare afiseaza mesajul "Do not worry. Ghosts do not exist!".

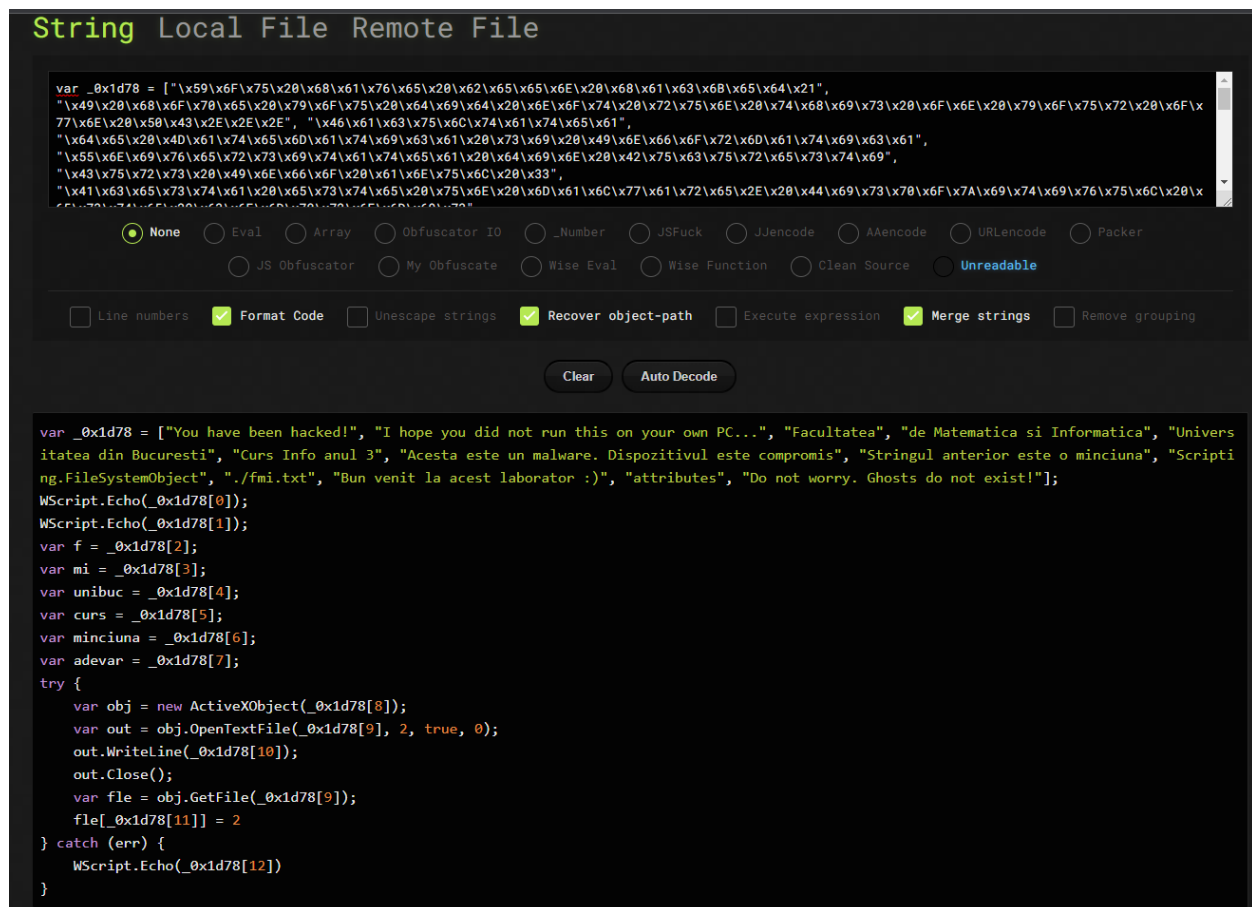
Fisierul nu este un malware deoarece, in mod evident, nu are scop malitios, acesta este menit doar sa afiseze niste mesaje sau/si sa creeze un fisier de tip txt inofensiv fiind realizat de o persoana in scop informativ.

### Exercitiul 3:

Am incercat sa rulez scriptul cu Microsoft Windows Based Script Host si am obtinut urmatoarele rezultate:



Dupa trecerea codului prin <https://lelinhtinh.github.io/de4js/> observam ca acesta are acelasi rol ca sample 2.



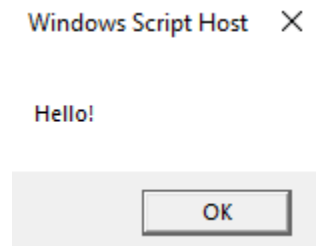
Codul nu ruleaza in vsc, dar observam ca acesta este scris direct in js. Mesajele acum sunt scrise in hexa.

Fata de codul din sample 2, acum mai avem si un array de stringuri, fiecare variabila avand un indice pentru un string din sirul definit la inceput.

'\x\$\$' reprezinta faptul ca valorile sunt scrise in hexa.

#### Exercitiul 4:

Am incercat sa rulez scriptul cu Microsoft Windows Based Script Host si am obtinut urmatoarele rezultate:



Daca convertim fiecare comentariu din base 64 in string obtinem urmatoarele:

hello world

this sample is a javascript

JavaScript sample

FMI UNIBUC

Facultatea de Matematica si Informatica

Felicitari

Universitatea din Bucuresti

Dezactivati antivirusul inainte de a rula acest exercitiu

unibuc in hex <- in hexa

Suspicios

Laborator

UNIBUC FMI

Universitatea din Bucuresti Facultatea de Matematica si Informatica

Acesta este un script

Acesta este un comentariu

Comentariu

Universitate

Run

Acest comentariu este ascuns <- 2x

Acest comentariu este ascuns <- 3x

Daca incercam sa convertim stringul din base64 din primul apel al functiei JSZQ92 obtinem ceva de genul:

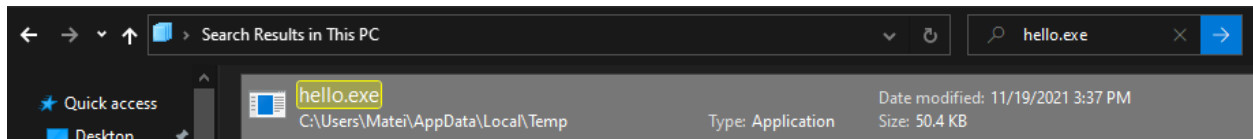
```
MZ@@@ !L!This program cannot be run in DOS mode.

$PEL@@<a@@@@@@@@,@@@@@P@@@@ pX@@@@Dq.text@@@@P'.data@@@@@0.rdata@@@@@0@/4
dP@@@@@0@.bssP`0.idataXp@$@0.CRT@@, @0.tls @. @0/14X@@@@@B/29UST2@@@@B/41c@@@@@B/55O@ @@@@@B/
6780@@@@0B/80@@@@@B@D$ =wN=s`=@@@@$@@@@H@@@@&1@@@@=tl=@=uD$@@@@@t$@n$D$@@$`@@uD
$@@@Gk'=@@UD$@@@@@tY@4$@n#@$@nD$@@@@$D$@@@@$D$@@@@t&'US@x@@@@tD$@D
$@@@f'@@@0@@@@@>$`@tBq@0@D$C@@$/@$`@D$C0$@@$`@D$C@P$@@@@@0@ @@@D$`
@D$@@@`@Q$@@@SM@'<D$,D$`@Q$`@D$,D$@@@0@DSD$(D$@@<D@@@q@t&'@@$@@q@t&'%q@v'%q@UV
S@@$@@@p@@@@$@@@7@@l'@D$@@@@@@7@@D$@@)@@@Q$"@@@@@tD$@@@`@Q$P@0@t:@$A@@@
@tD$@@O@@@@$
@@t @Q$0@Q$0@Q$e[^\]v@@ @ @
U@@@t @P@Cl'@t@@$
```

Observam ca toate cele 4 apeluri ale functiei incep cu "MZ———  
@ !L!This program cannot be run in DOS mode."

Observam din analiza statica faptul ca sample-ul incearca sa execute un try care vrea sa creeze un obiect cu ajutorul functiei JSZQ99, si sa scrie ceva in acest obiect, dupa care sa il lase in calculator(un executabil), dar prinde o eroare, deci afiseaza doar "Hello!".

Teoretic programul este malware, deoarece el instaleaza in calculator un .exe.



Din fericire, acest executabil este inofensiv.



Site-ul VirusTotal detecteaza fisierul ca fiind un malware.

21

/ 57

?

Community Score

21 security vendors flagged this file as malicious

a196ea13937f9b858c9fb2a5e6ecf139d324a022cbd21adcc217f7e581a73e21

sample4.js

text

3.39 MB

Size

2021-11-18 16:27:46 UTC

22 hours ago

TXT

DETECTION	DETAILS	COMMUNITY
Ad-Aware	JS.Heur.Cbum.1.64A98D8B.Gen	ALYac
Arcabit	JS.Heur.Cbum.1.64A98D8B.Gen	Avast
AVG	VBS:Downloader-ANE [Trj]	BitDefender
Cyren	JS/Nemucod.N!Eldorado	DrWeb
Emsisoft	JS.Heur.Cbum.1.64A98D8B.Gen (B)	eScan
FireEye	JS.Heur.Cbum.1.64A98D8B.Gen	Fortinet
GData	JS.Heur.Cbum.1.64A98D8B.Gen	Ikarus
Kaspersky	HEUR:Trojan-Dropper.Script.Generic	Lionic
MAX	Malware (ai Score=84)	Microsoft
NANO-Antivirus	Trojan.Script.Ransom.dqzgwv	Sangfor Engine Zero
Symantec	Trojan.Gen.NPE	AhnLab-V3
Antiy-AVL	Undetected	Avira (no cloud)

Observam ca dupa obfuscarea fisierului, numarul de flaguri a scazut drastic, acesta continuand sa fie semnalat ca malware.

3

/ 57

?

Community Score

3 security vendors flagged this file as malicious

4d6bd936cb25a2111392b84ba13077bd87c24309e57ae8c2f9914119776278d

sample41.js

text

3.27 MB

Size

2021-11-03 03:05:01 UTC

16 days ago

TXT

DETECTION	DETAILS	COMMUNITY
DrWeb	Trojan.MulDrop18.46723	Kaspersky
ZoneAlarm by Check Point	HEUR:Trojan-Dropper.Script.Generic	Ad-Aware
AhnLab-V3	Undetected	ALYac
Antiy-AVL	Undetected	Arcabit
Avast	Undetected	Avira (no cloud)
Baidu	Undetected	BitDefender
BitDefenderTheta	Undetected	Bkav Pro
CAT-QuickHeal	Undetected	ClamAV
CMC	Undetected	Comodo
Cynet	Undetected	Cyren
Emsisoft	Undetected	eScan
ESET-NOD32	Undetected	F-Secure
FireEye	Undetected	Fortinet
GData	Undetected	Gridinsoft