Laborator 4

Securitatea Sistemelor Informatice

1.

A -> 4

B -> 2

C -> 1

D -> 3

 $E \rightarrow 6$

 $F \rightarrow 5$

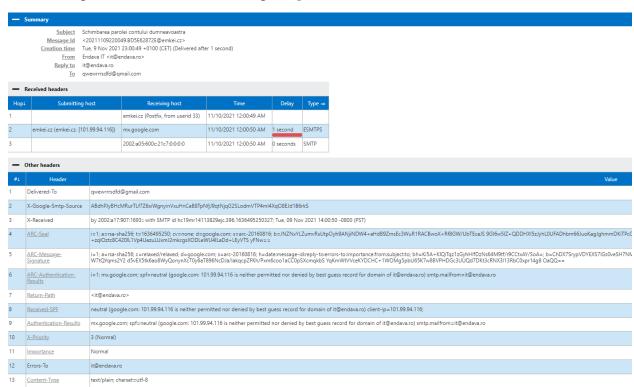
2.

- Titlul este "mesaj important".
- Email-ul a fost catalogat drept "junk" de catre serviciul de mail folosit.
- Sender-ul este "Home bank.ro", neavand legatura cu ing.ro.
- Email-ul este primit de la mbm@externalys.net, nu de la o adresa cu numele de domeniu ing.ro.
- Aspect neingrijit al textului. (ex: litera mica la inceputul unui paragraph, "Telefon" scris pe un rand, iar numarul scris pe urmatorul etc.)
- Email-ul nu este semnat de o persoana concreta, ci de "ING Bank Romania".
- In email apare link-ul "zozweb,com/RRO", care nu are legatura cu ing.ro.

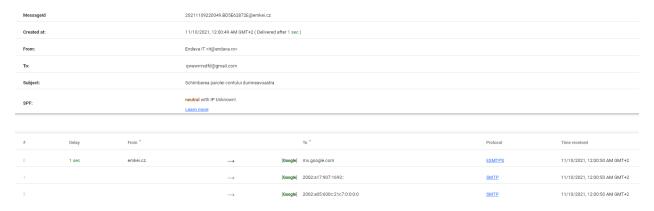
Am folosit urmatorul email (catre un angajat al firmei Endava):

From Name:	Endava IT
From E-mail:	it@endava.ro
To:	qwewrrrsdfd@gmail.com
Subject:	Schimbarea parolei contului dumneavoastra
Attachment:	Choose File No file chosen
	Attach another file
	Advanced Settings
Content-Type:	● text/plain
Text:	Bună ziua!
	A fost sesizată o încercare de a schimba parola contului dumneavoastră de institutional. Pentru a ne asigura că dumneavoastră ati încercat să faceti această schimbare, completati următorul formular cu numele si parola contului dumneavoastră: formular.com Odată completat acest formular, veti primi un email de schimbare a parolei. O zi frumoasă, Echipa IT Endava. Solve reCAPTCHA v2 instead of v3
	Send Clear

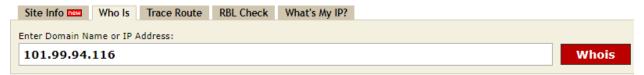
Rezultat dupa introducerea header-ului pe https://mha.azurewebsites.net/:



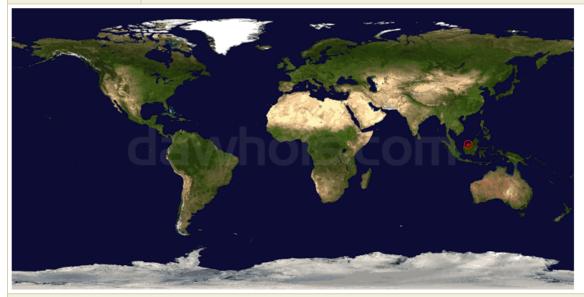
Rezultat dupa introducerea header-ului pe https://toolbox.googleapps.com/apps/messageheader/:



Rezultat dupa introducerea IP-ului pe https://dawhois.com/:



101.99.94.116 - Geo Information	
IP Address	101.99.94.116
Host	emkei.cz
Location	MY, Malaysia
City	-,
Organization	Piradius Net
ISP	Piradius Net
Latitude	2°50'00" North
Longitude	112°50'00" East
Distance	9751.91 km (6059.56 miles)
Map Location ™	



101.99.94.116 - Whois Information

Raspunsuri pentru intrebari:

- Daca atacul ar fi cu success, as obtine datele unei persoane din firma Endava si as putea obtine informatii confidentiale din interiorul firmei.

- SPF pentru email-ul trimis: *NEUTRAL cu adresa IP 101.99.94.116* SPF pentru un email legitim: *PASS cu adresa IP 172.82.230.59*

DKIM pentru email-ul trimis: -

DKIM pentru un email legitim: 'PASS' cu domeniul m1.email.samsung.com

DMARC pentru email-ul trimis: -

DMARC pentru un email legitim: 'PASS'