

Министерство образования республики Молдова
Технический Университет Молдовы
Департамент Программной Инженерии и Автоматики

О т ч ё т

Лабораторная работа №4

По предмету: Infractioni informatice si tehnici de investigare

Выполнил студ. гр. SI-202

Абабий Эдуард

Проверил

Масютин Максим

Кишинёв – 2023

Scopul acestui laborator este de a-i învăța pe studenți să identifice și să analizeze artefacte email.

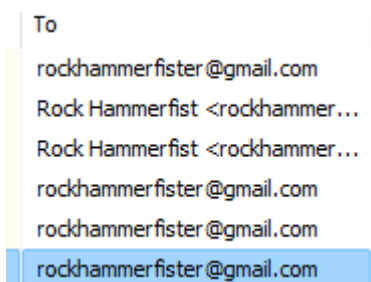
Sarcina:

1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierului email!
2. Pentru 3 întrebări, de mai jos, selectate la dorință, creați un writeup (descrieți pe pași cum ați aflat răspuns la întrebările selectate, obligatoriu includeți și capturi de ecran).

Rezolvarea sarcinilor:

1. Ce adresă email a fost folosită?

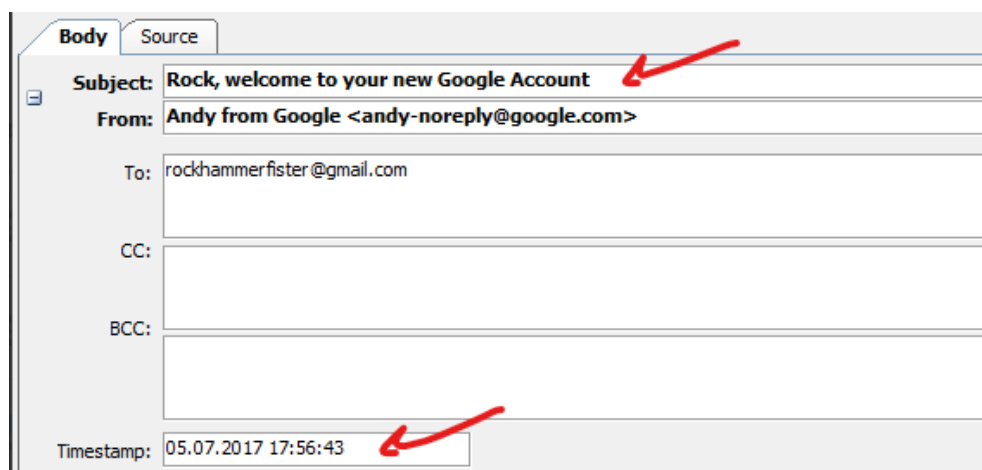
rockhammerfister@gmail.com

A screenshot of an email interface showing a list of recipients under the 'To' field. The list contains five entries, all of which are 'rockhammerfister@gmail.com'. The last entry is highlighted with a blue selection bar.

To
rockhammerfister@gmail.com
Rock Hammerfist <rockhammer...
Rock Hammerfist <rockhammer...
rockhammerfister@gmail.com
rockhammerfister@gmail.com
rockhammerfister@gmail.com

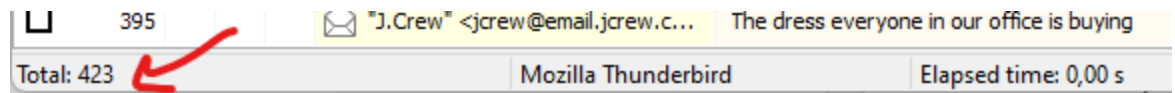
2. Când a fost aceasta configurată pentru prima oară?

5 июля 2017 года в 17:56:43



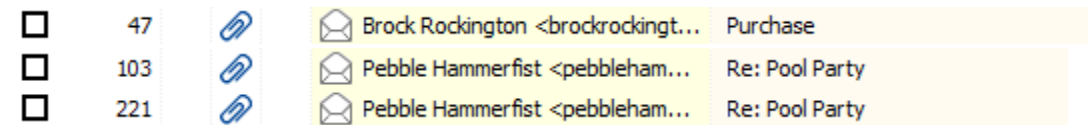
3. Câte mesaje au fost în inbox?

423



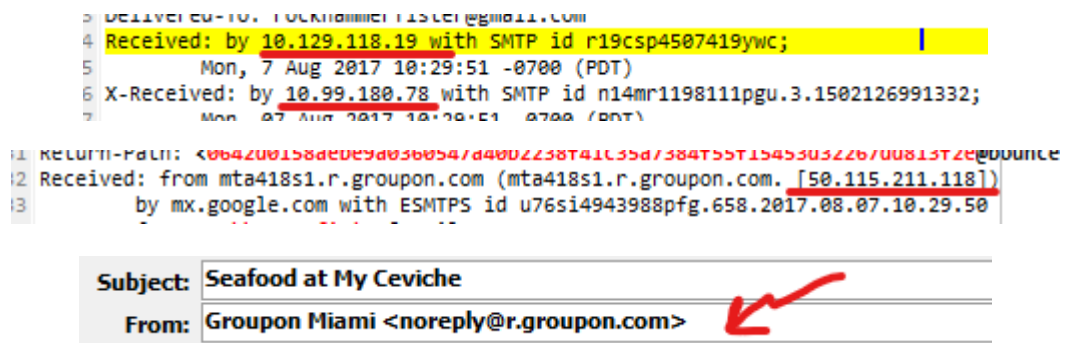
4. Câte mesaje au atașamente?

3



5. Localizați mesajul 416 și deschideți-l. Click pe fila sursei. Ce adrese IP a traversat acest mesaj? De la cine a fost acest email?

Сообщение было от noreply@r.groupon.com , 10.129.118.19 / 10.99.180.78 / 50.115.211.118



6. Cu cine dintre cei care nu erau prezenți pe lista de adresați utilizatorul a discutat cel mai mult?

pebblehammerfist@aol.com Pebble Hammerfist

All Mail

Drafts

Trash

Important

Filter: From

pebblehammerfist@aol.com


	#	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	From	Subject
<input type="checkbox"/>	39			<div></div> Pebble Hammerfist <pebbleham...	Re: Joined SecondLife
<input type="checkbox"/>	40			<div></div> Pebble Hammerfist <pebbleham...	Re: Help - my PC is running slow!
<input type="checkbox"/>	41	<div></div>		<div></div> Pebble Hammerfist <pebbleham...	Re: Pool Party
<input type="checkbox"/>	11			<div></div> Pebble Hammerfist <pebbleham...	Re: My business trip
<input type="checkbox"/>	5			<div></div> pebblehammerfist@aol.com	Retirement

7. Au fost oricare membri ai familiei în orice conversație? (Sugestie: folosiți capacitățile de filtru.)

pebblehammerfist@aol.com Pebble Hammerfist


Filter: From		hammer					
	#	↑↓	📎	▶	From	Subject	
<input type="checkbox"/>	219				📧 Pebble Hammerfist <pebbleham...	Re: Joined SecondLife	
<input type="checkbox"/>	105				📧 Pebble Hammerfist <pebbleham...	Re: Joined SecondLife	
<input type="checkbox"/>	220				📧 Pebble Hammerfist <pebbleham...	Re: Help - my PC is running slow!	
<input type="checkbox"/>	104				📧 Pebble Hammerfist <pebbleham...	Re: Help - my PC is running slow!	
<input type="checkbox"/>	221		📎		📧 Pebble Hammerfist <pebbleham...	Re: Pool Party	
<input type="checkbox"/>	103		📎		📧 Pebble Hammerfist <pebbleham...	Re: Pool Party	
<input type="checkbox"/>	102				📧 Pebble Hammerfist <pebbleham...	Re: Going Back to Arkham	
<input type="checkbox"/>	101				📧 Pebble Hammerfist <pebbleham...	Re: This Game is soooo addicting!	
<input type="checkbox"/>	44				📧 Pebble Hammerfist <pebbleham...	Re: My business trip	
<input type="checkbox"/>	12				📧 pebblehammerfist@aol.com	Retirement	

8. Să ne concentrăm asupra email-urilor de la Brock Rockigton. Câte astfel de email-uri au fost? (Sugestie: folosiți capacitățile de filtru.)

Filter: From		brockrockington@yahoo.com			
#			From	Subject	
<input type="checkbox"/>	322		Brock Rockington <brockrockingt...	Re: Beer links	
<input type="checkbox"/>	323		Brock Rockington <brockrockingt...	Re: Beer links	
<input type="checkbox"/>	321		Brock Rockington <brockrockingt...	Re: Beer links	
<input type="checkbox"/>	320		Brock Rockington <brockrockingt...	Re: Beer links	
<input type="checkbox"/>	318		Brock Rockington <brockrockingt...	Re: Beer links	
<input type="checkbox"/>	224		Brock Rockington <brockrockingt...	Re: Beer links	
<input type="checkbox"/>	319		Brock Rockington <brockrockingt...	Beer links	
<input type="checkbox"/>	223		Brock Rockington <brockrockingt...	Beer links	
<input type="checkbox"/>	217		Brock Rockington <brockrockingt...	Re: Best Beatles cover - EVER!	
<input type="checkbox"/>	109		Brock Rockington <brockrockingt...	Re: Best Beatles cover - EVER!	
<input type="checkbox"/>	218		Brock Rockington <brockrockingt...	Re: you won't believe all these pale ales!	
<input type="checkbox"/>	107		Brock Rockington <brockrockingt...	Re: you won't believe all these pale ales!	
<input type="checkbox"/>	57		Brock Rockington <brockrockingt...	Re: Dry Erase Solvent	
<input type="checkbox"/>	56		Brock Rockington <brockrockingt...	Re: Do you remember your Latin?	
<input type="checkbox"/>	47		Brock Rockington <brockrockingt...	Purchase	
<input type="checkbox"/>	48		Brock Rockington <brockrockingt...	Re: We Can Skip the Gym Today	
<input type="checkbox"/>	45		Brock Rockington <brockrockingt...	Re: Laying tile	
<input type="checkbox"/>	43		Brock Rockington <brockrockingt...	Laying tile	
<input type="checkbox"/>	42		Brock Rockington <brockrockingt...	Re: URL	
<input type="checkbox"/>	14		Brock Rockington <brockrockingt...	Re: Happy Hour	
<input type="checkbox"/>	13		Brock Rockington <brockrockingt...	Re: Happy Hour	
<input type="checkbox"/>	3		Brock Rockington <brockrockingt...	Re: Router	
Total: 423 Visible: 22			Mozilla Thunderbird		Elapsed time: 0,02 s

a. A avut ataşament oricare dintre aceste mesaje?

Да, на фотографии выше видно, что 47 сообщение имеет прикреплённый материал

<input type="checkbox"/>	47		Brock Rockington <brockrockingt...	Purchase
--------------------------	----	---	------------------------------------	----------

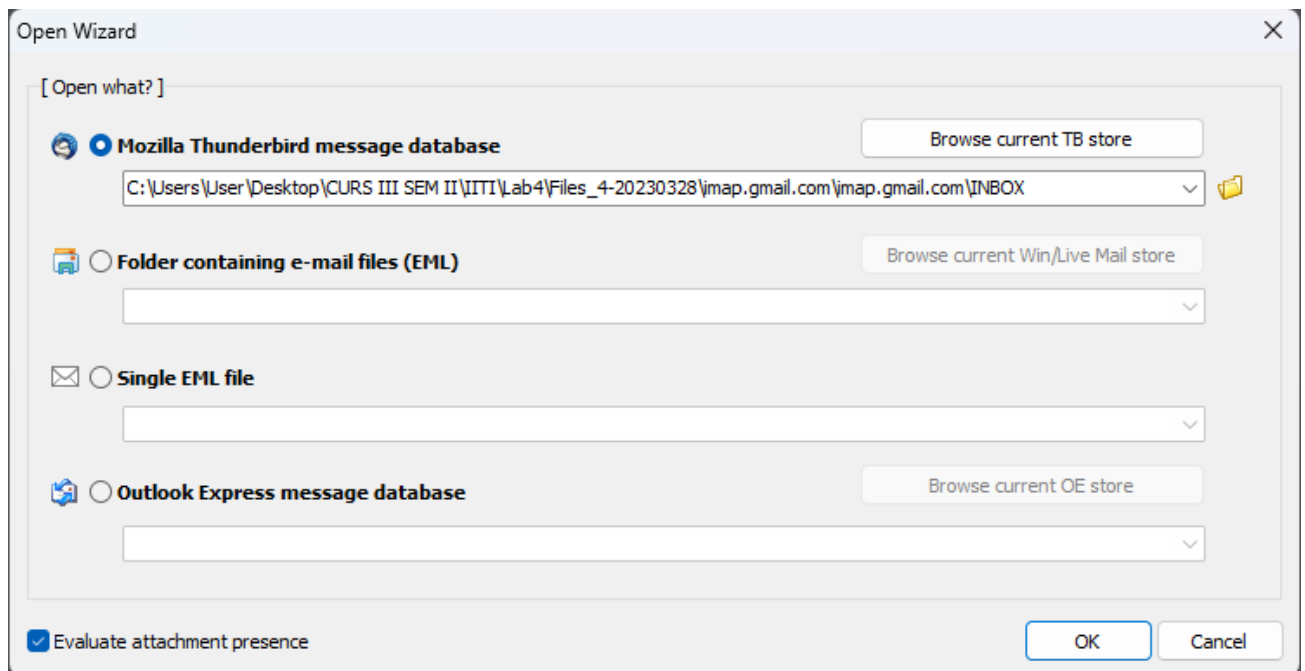
- b. Au fost transmise între aceste două persoane link-uri care să prezinte valoare pentru anchetă? Care este marca temporală? Ceva din laboratorul nostru dedicat internetului? (Sugestie: adăugați în cronologie)

Brock Rockington отправил ссылку направленную на exe файл скрытую под меню с напитками

```
45 aPe=3D"rect" id=3D"y1v62//512426m_-50/1016804456461269y1v1184908586y01=
46 _3_16_0_ym19_1_1500995456007_11465" target=3D"_blank" href=3D"http://w=
47 ww.caboosebrewing.com/drinks/">http://www.caboosebrewing.com/ drinks/b=
48 eerlist.exe</a><br clear=3D"none">
49 </div>
```

2. Writeup: Întrebarea 1, 2, 3.

Открываем файл с данными через программу Mail Viewer



Na открывшейся странице уже видим ответ на первые 2 вопроса, это сколько сообщений всего, можно посмотреть в левом нижнем углу и когда был создан аккаунт

INBOX						
Filter: <input type="text"/> <input type="text"/>						
	#		From	Subject	To	Received
<input type="checkbox"/>	1		Andy from Google <andy-norepl...>	Rock, welcome to your new Google ...	rockhammerfister@gmail.com	05.07.
<input type="checkbox"/>	2		Broadlands HOA Forums <DoNot...>	Broadlands HOA Discussion Forum A...	Rock Hammerfist <rockhammer...>	05.07.
<input type="checkbox"/>	3		Brock Rockington <brockrockingt...>	Re: Router	Rock Hammerfist <rockhammer...>	06.07.
<input type="checkbox"/>	4		Groupon <notify@r.groupon.com>	Welcome!	rockhammerfister@gmail.com	06.07.
<input type="checkbox"/>	5		"J.Crew" <jcrew@email.jcrew.c...>	Say hello to your 15% off code	rockhammerfister@gmail.com	06.07.
<input type="checkbox"/>	8		500px <info@500px.com>	500px Step 1: Please confirm your ...	rockhammerfister@gmail.com	06.07.
<input type="checkbox"/>	7		Banana Republic Factory <bana...>	Your welcome gift is here!	rockhammerfister@gmail.com	06.07.
<input type="checkbox"/>	6		Gap <gap@email.gap.com>	Just for you, a special welcome from...	rockhammerfister@gmail.com	06.07.
<input type="checkbox"/>	11		Groupon Miami <noreply@r.grou...>	Mani-Pedis	rockhammerfister@gmail.com	07.07.
<input type="checkbox"/>	10		Groupon <noreply@r.groupon.c...>	Get More Bang for Your Buck	rockhammerfister@gmail.com	07.07.
<input type="checkbox"/>	9		500px <info@500px.com>	Meet your July Guest Editors, Cyclin...	rockhammerfister@gmail.com	07.07.
<input type="checkbox"/>	12		pebblehammerfist@aol.com	Retirement	rockhammerfister@gmail.com	07.07.
<input type="checkbox"/>	13		Brock Rockington <brockrockingt...>	Re: Happy Hour	Rock Hammerfist <rockhammer...>	07.07.
<input type="checkbox"/>	14		Brock Rockington <brockrockingt...>	Re: Happy Hour	Rock Hammerfist <rockhammer...>	07.07.
<input type="checkbox"/>	15		Groupon Miami <noreply@r.grou...>	Brunch	rockhammerfister@gmail.com	08.07.
<input type="checkbox"/>	16		"J.Crew" <jcrew@email.jcrew.c...>	Hello, style	rockhammerfister@gmail.com	08.07.
<input type="checkbox"/>	17		Old Navy <oldnavy@email.oldna...>	Now that you're part of the family...	rockhammerfister@gmail.com	08.07.
<input type="checkbox"/>	18		Groupon Experiences <noreply...>	Miami Marlins International Champi...	rockhammerfister@gmail.com	08.07.
<input type="checkbox"/>	19		Groupon <noreply@r.groupon.c...>	\$10 OFF with Code	rockhammerfister@gmail.com	09.07.
<input type="checkbox"/>	20		Groupon Miami <noreply@r.grou...>	Sunday Brunch	rockhammerfister@gmail.com	09.07.
<input type="checkbox"/>	21		Athleta <athleta@email.athleta....>	No, For Real. Give it the Sweat Test.	rockhammerfister@qmail.com	09.07.
Total: 423						
Mozilla Thunderbird						

А немного полистав, мы находим, что только 3 сообщения имели вложенный материал.

Вывод: В этой лабораторной работе я научился анализировать электронную почту. Узнал, как просмотреть с кем цель общалась, какие предпочтения, откуда чаще всего приходятся уведомления. Также анализировать письма на отправку вредоносных файлов и поиск потенциальных злоумышленников.