Министерство образования республики Молдова

Технический Университет Молдовы

Департамент Программной Инженерии и Автоматики

Отчёт

Лабораторная работа №4

По предмету: Infractiuni 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:**

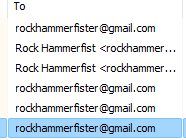
1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierului email!

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:**

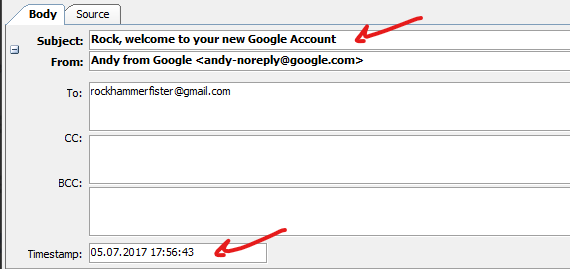
1. Ce adresă email a fost folosită?

rockhammerfister@gmail.com



1. Când a fost aceasta configurată pentru prima oară?

5 июля 2017 года в 17:56:43



1. Câte mesaje au fost în inbox?

423

1. Câte mesaje au atașamente?

3





1. 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](mailto:noreply@r.groupon.com) , 10.129.118.19 / 10.99.180.78 / 50.115.211.118

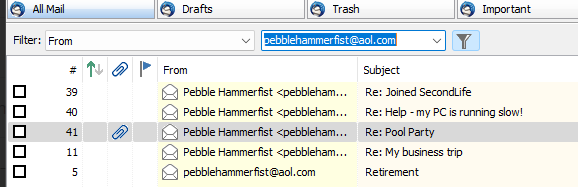






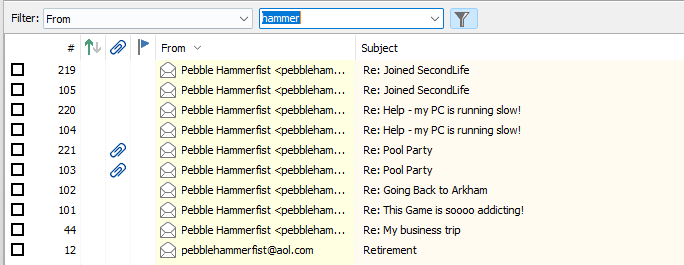
1. Cu cine dintre cei care nu erau prezenți pe lista de adresați utilizatorul a discutat cel mai mult?

[pebblehammerfist@aol.com](mailto:pebblehammerfist@aol.com) Pebble Hammerfist



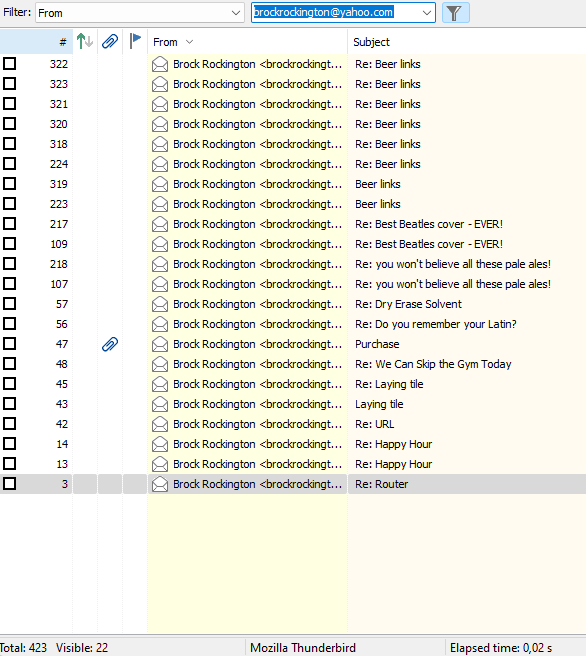
1. Au fost oricare membri ai familiei în orice conversație? (Sugestie: folosiți capacitățile de filtru.)

[pebblehammerfist@aol.com](mailto:pebblehammerfist@aol.com) Pebble Hammerfist



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

22



* 1. A avut atașament oricare dintre aceste mesaje?

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



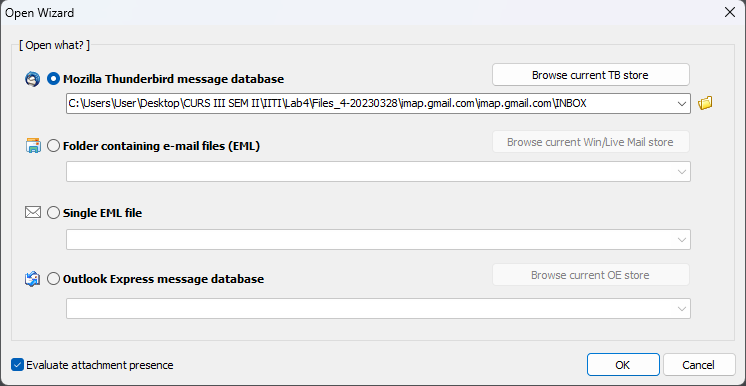
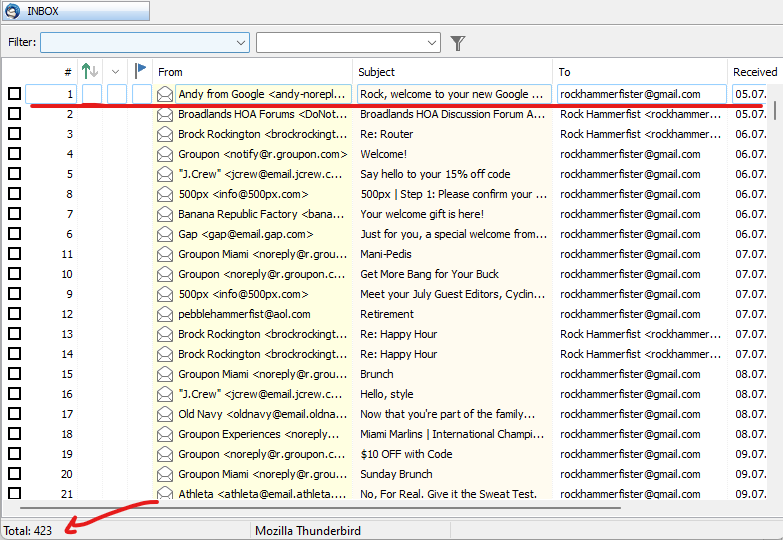
* 1. Au fost transmise între aceste două persoane link-uri care să prezinte valoare pentru anchetă? Care este marca temporală? Ceva din laboratorul nostru dedicat internetului? (Sugestie: adăugați în cronologie)

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



**2. Writeup: Întrebarea 1, 2, 3.**

Открываем файл с данными через программу Mail Viewer

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


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.