Министерство образования республики Молдова

Технический Университет Молдовы

Департамент Программной Инженерии и Автоматики

Отчёт

Лабораторная работа №3

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 extragă și să analize artefacte internet relevante.

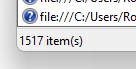
**Sarcina:**

1. Completați cîmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor.

**Rezolvarea sarcinilor:**

1. Câte artefacte unice identificați?

1517



1. Ce site a fost vizitat cel mai mult (ignoră “about:blank”)?

https://www.google.com/?gws\_rd=ssl



1. Au fost careva căutări Google suspecte?

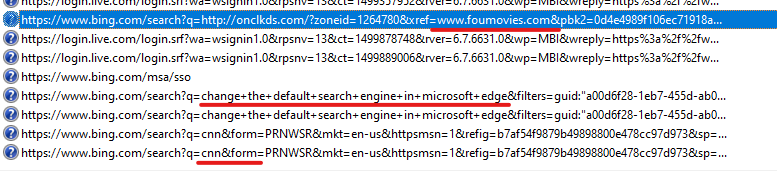
Tnt explosive , Bikini pool party





1. Ce termeni au fost căutați folosind Bing?

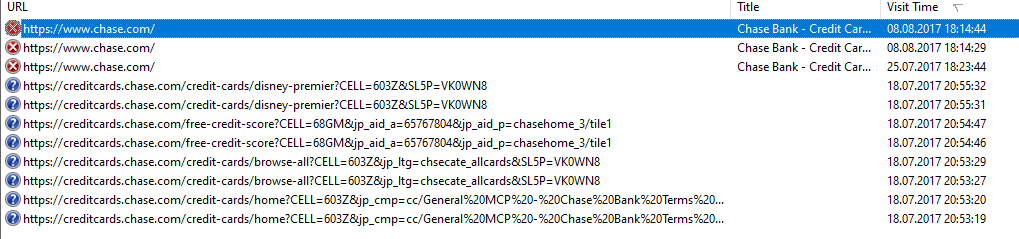
[www.fourmovies.com](http://www.fourmovies.com) / change the default search engine in Microsoft edge / cnn



1. Ce conturi bancare a deținut aparent utilizatorul? Când au fost vizitate aceste site-uri?

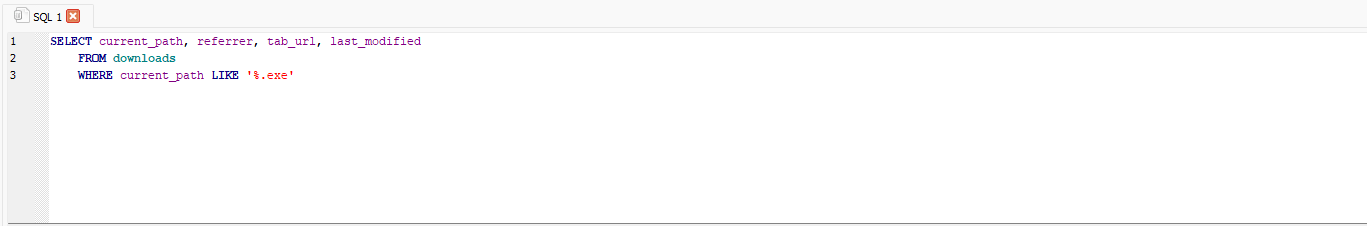
Пользователь использовал банковский счёт в банке Chase Bank, использовал сайт chase.com

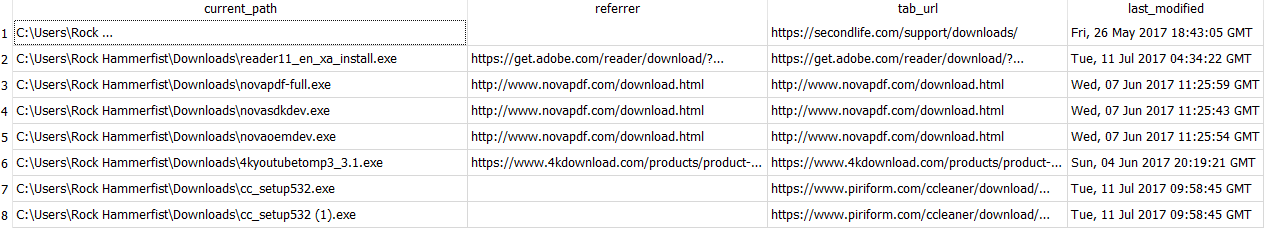
Последнее посещение сайта было 08.08.2017 18:14:44



1. În ce zi și la ce oră au fost descărcate toate executabilele? Ce nume de fișier au avut acestea?

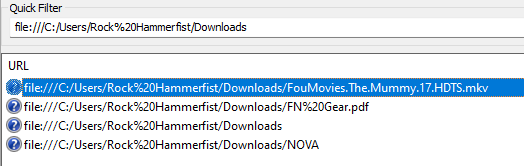
На фотографии ниже предоставлен список файлов .exe которые были скачаны из интернета





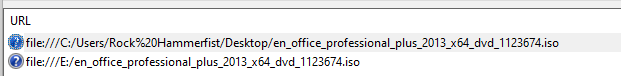
1. Ce conținut a fost accesat din directoriul Downloads?

Ниже на фотографии предоставлены файлы открытые в браузере из папки Downloads



1. Au fost careva fișiere accesate din medii detașabile? Care au fost acestea?

Был использован только iso образ en\_office\_professional\_plus\_2013\_x64\_dvd\_1123674.iso



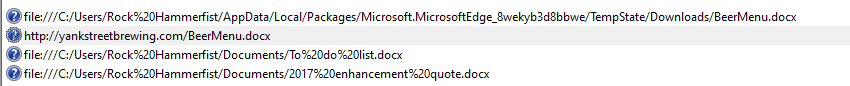
1. Puteți spune dacă utilizatorul are conturi webmail? Dacă da, care anume?

Да, пользователь имеет почту gmail и Microsoft mail



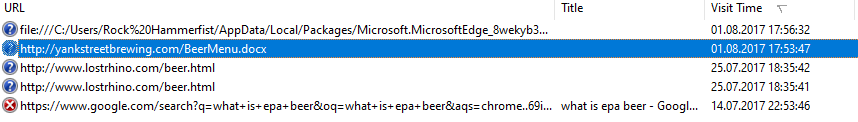
1. Câte documente word au fost accesate?

Были использованы 4 документа word (.docx)



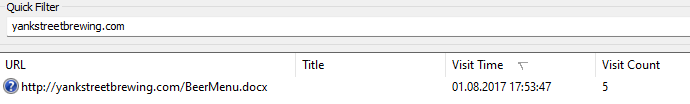
1. Câte site-uri de bere/producere a berii au fost vizitate? În ce interval de timp?

Пользователем были посещены 3 сайта с ключевым словом beer с интервалом от 14 июля 2017 года – 1 августа 2017 года



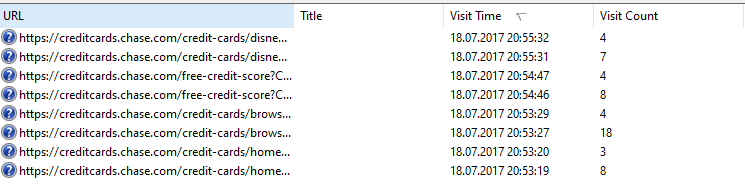
1. De câte ori utilizatorul a vizitat *yankstreetbrewing.com*? Ce a fost accesat? Când? Ce ați dori să faceți în calitate de următoarea acțiune criminalistică cu aceste informații? (Sugestie: Adăugați asta la cronologie.)

Сайт *yankstreetbrewing.com* посещался пользователем **5** раз и именно раздел с меню.  
Исходя из полученной информации, как злоумышленник я бы создал файл или картинку с названием *yankstreetbrewing\_new\_menu.png* или *.pdf* в котором будет находиться вирус.  
Также можно создать фейковую страницу *yankstreetbrewing* где можно будет разместить акцию о том, что купив 2 пива онлайн – доставка и 1 пиво в подарок бесплатно. Таким образом можно будет украсть данные его карты.



1. A avut loc o vizită bancară după această dată și timp? Când? (Sugestie: Adăugați asta la cronologie.)

Все посещения сайта банка были в июле 18.07.2017 года



Вывод: В данной лабораторной работе я изучил способ просмотра и поиска информации с историей браузера. Как просмотреть и получить данные о скачанных файлах, просмотреть время, когда всё это было сделано и разработать план по атаке этого пользователя.