

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

О т ч ё т

Лабораторная работа №3

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 extragă și să analizeze artefacte internet relevante.

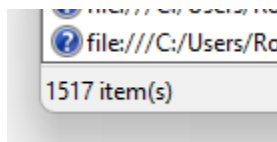
Sarcina:

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

Rezolvarea sarcinilor:

1. Câte artefacte unice identificați?

1517



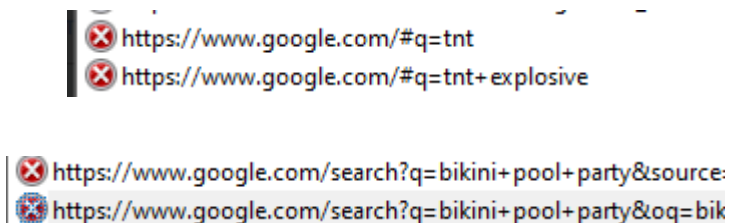
2. Ce site a fost vizitat cel mai mult (ignoră "about:blank")?

https://www.google.com/?gws_rd=ssl

URL	FILE	VISIT DATE	VISIT COUNT
about:blank		01.08.2017 17:56:28	2021
https://www.google.c...		05.07.2017 17:46:33	154
javascript:false		14.07.2017 19:36:07	152

3. Au fost careva căutări Google suspecte?

Tnt explosive , Bikini pool party



4. Ce termeni au fost căutați folosind Bing?

www.fourmovies.com / change the default search engine in Microsoft edge / cnn

https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1499878748&rver=6.7.6631.0&wp=MBI&wreply=https%3a%2f%2fw...
https://www.bing.com/search?q=http://onclks.com/?zoneid=1264780&xref=www.fourmovies.com&pbk2=0d4e4989f106ec71918a...
https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1499878748&rver=6.7.6631.0&wp=MBI&wreply=https%3a%2f%2fw...
https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1499889006&rver=6.7.6631.0&wp=MBI&wreply=https%3a%2f%2fw...
https://www.bing.com/msa/sso
https://www.bing.com/search?q=change+the+default+search+engine+in+microsoft+edge&filters=guid:"a00d6f28-1eb7-455d-ab0...
https://www.bing.com/search?q=change+the+default+search+engine+in+microsoft+edge&filters=guid:"a00d6f28-1eb7-455d-ab0...
https://www.bing.com/search?q=cnn&form=PRNWSR&mkt=en-us&httpsmsn=1&refig=b7af54f9879b49898800e478cc97d973&sp=...
https://www.bing.com/search?q=cnn&form=PRNWSR&mkt=en-us&httpsmsn=1&refig=b7af54f9879b49898800e478cc97d973&sp=...

5. 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

URL	Title	Visit Time
https://www.chase.com/	Chase Bank - Credit Car...	08.08.2017 18:14:44
https://www.chase.com/	Chase Bank - Credit Car...	08.08.2017 18:14:29
https://www.chase.com/	Chase Bank - Credit Car...	25.07.2017 18:23:44
https://creditcards.chase.com/credit-cards/disney-premier?CELL=603Z&SL5P=VK0WN8		18.07.2017 20:55:32
https://creditcards.chase.com/credit-cards/disney-premier?CELL=603Z&SL5P=VK0WN8		18.07.2017 20:55:31
https://creditcards.chase.com/free-credit-score?CELL=68GM&jp_aid_a=657678048&jp_aid_p=chasehome_3/tile1		18.07.2017 20:54:47
https://creditcards.chase.com/free-credit-score?CELL=68GM&jp_aid_a=657678048&jp_aid_p=chasehome_3/tile1		18.07.2017 20:54:46
https://creditcards.chase.com/credit-cards/browse-all?CELL=603Z&jp_ltg=chsecate_allcards&SL5P=VK0WN8		18.07.2017 20:53:29
https://creditcards.chase.com/credit-cards/browse-all?CELL=603Z&jp_ltg=chsecate_allcards&SL5P=VK0WN8		18.07.2017 20:53:27
https://creditcards.chase.com/credit-cards/home?CELL=603Z&jp_cmp=cc/General%20MCP%20-%20Chase%20Bank%20Terms%20...		18.07.2017 20:53:20
https://creditcards.chase.com/credit-cards/home?CELL=603Z&jp_cmp=cc/General%20MCP%20-%20Chase%20Bank%20Terms%20...		18.07.2017 20:53:19

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

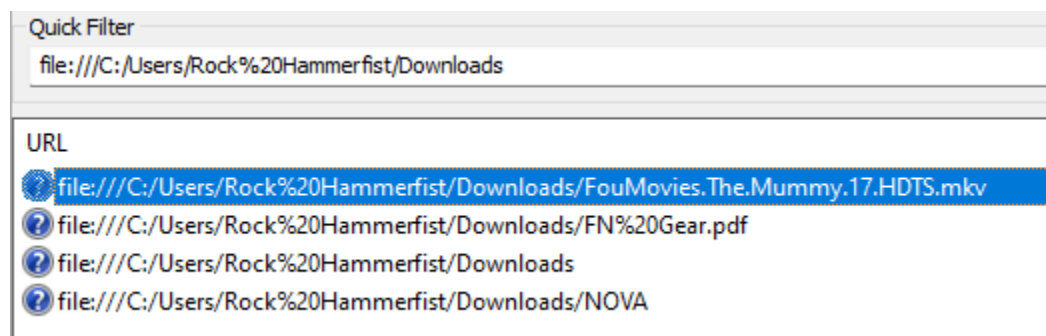
На фотографии ниже предоставлен список файлов .exe которые были скачаны из интернета

```
SQL 1
1 SELECT current_path, referrer, tab_url, last_modified
2 FROM downloads
3 WHERE current_path LIKE '%.exe'
```

	current_path	referrer	tab_url	last_modified
1	C:\Users\Rock ...		https://secondlife.com/support/downloads/	Fri, 26 May 2017 18:43:05 GMT
2	C:\Users\Rock Hammerfist\Downloads\reader11_en_xa_install.exe	https://get.adobe.com/reader/download/?...	https://get.adobe.com/reader/download/?...	Tue, 11 Jul 2017 04:34:22 GMT
3	C:\Users\Rock Hammerfist\Downloads\novapdf-full.exe	http://www.novapdf.com/download.html	http://www.novapdf.com/download.html	Wed, 07 Jun 2017 11:25:59 GMT
4	C:\Users\Rock Hammerfist\Downloads\novasdkdev.exe	http://www.novapdf.com/download.html	http://www.novapdf.com/download.html	Wed, 07 Jun 2017 11:25:43 GMT
5	C:\Users\Rock Hammerfist\Downloads\novaoemdev.exe	http://www.novapdf.com/download.html	http://www.novapdf.com/download.html	Wed, 07 Jun 2017 11:25:54 GMT
6	C:\Users\Rock Hammerfist\Downloads\4koutubetomp3_3.1.exe	https://www.4kdownload.com/products/product-...	https://www.4kdownload.com/products/product-...	Sun, 04 Jun 2017 20:19:21 GMT
7	C:\Users\Rock Hammerfist\Downloads\cc_setup532.exe		https://www.piriform.com/ccleaner/download/...	Tue, 11 Jul 2017 09:58:45 GMT
8	C:\Users\Rock Hammerfist\Downloads\cc_setup532 (1).exe		https://www.piriform.com/ccleaner/download/...	Tue, 11 Jul 2017 09:58:45 GMT

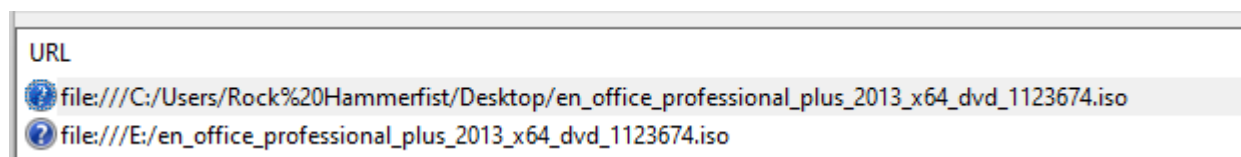
7. Ce conținut a fost accesat din directoriul Downloads?

Ниже на фотографии предоставлены файлы открытые в браузере из папки Downloads



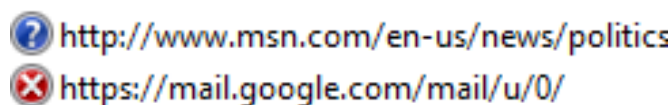
8. Au fost careva fișiere accesate din medii detașabile? Care au fost acestea?

Был использован только iso образ en_office_professional_plus_2013_x64_dvd_1123674.iso



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

Да, пользователь имеет почту gmail и Microsoft mail



10. Câte documente word au fost accesate?

Были использованы 4 документа word (.docx)

file:///C:/Users/Rock%20Hammerfist/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/BeerMenu.docx
http://yankstreetbrewing.com/BeerMenu.docx
file:///C:/Users/Rock%20Hammerfist/Documents/To%20do%20list.docx
file:///C:/Users/Rock%20Hammerfist/Documents/2017%20enhancement%20quote.docx

11. 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

URL	Title	Visit Time
file:///C:/Users/Rock%20Hammerfist/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3...		01.08.2017 17:56:32
http://yankstreetbrewing.com/BeerMenu.docx		01.08.2017 17:53:47
http://www.lostrhino.com/beer.html		25.07.2017 18:35:42
http://www.lostrhino.com/beer.html		25.07.2017 18:35:41
https://www.google.com/search?q=what+is+epa+beer&oq=what+is+epa+beer&aqs=chrome..69i...	what is epa beer - Googl...	14.07.2017 22:53:46









12. 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.

Quick Filter			
yankstreetbrewing.com			
URL	Title	Visit Time	Visit Count
http://yankstreetbrewing.com/BeerMenu.docx		01.08.2017 17:53:47	5

13. 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

URL	Title	Visit Time	Visit Count
 https://creditcards.chase.com/credit-cards/disne...		18.07.2017 20:55:32	4
 https://creditcards.chase.com/credit-cards/disne...		18.07.2017 20:55:31	7
 https://creditcards.chase.com/free-credit-score?C...		18.07.2017 20:54:47	4
 https://creditcards.chase.com/free-credit-score?C...		18.07.2017 20:54:46	8
 https://creditcards.chase.com/credit-cards/brows...		18.07.2017 20:53:29	4
 https://creditcards.chase.com/credit-cards/brows...		18.07.2017 20:53:27	18
 https://creditcards.chase.com/credit-cards/home...		18.07.2017 20:53:20	3
 https://creditcards.chase.com/credit-cards/home...		18.07.2017 20:53:19	8

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.