Градусы и минуты

The condition of a given task:

`Где расположено это место 33.357778S, 151.442750E? Переведите координаты в минуты и секунды. Напишите краткий гайд о том, как вы это сделали, какими ресурсами пользовались.`

Solution:

input data is `33.357778S, 151.442750E` answer in this url minute and second conversion in same site btw **33°21'28.0"S 151°26'33.9"E**

Answer is ***9 Bon-Mace Cl, Berkeley Vale NSW 2261, Австралия and coordinates is 33°21'28.0"S 151°26'33.9"E***

Извлекаем MAC из PCAP

The condition of a given task:

`Укажите MAC-адрес компьютера с IP-адресом 192.168.0.8. В ответе укажите адрес в формате A0:B1:C2:D3:E4:F5.`

Solution:

Load the pcap dump to *wireshark/shark/tcpdump* and search by ***ip.src == 192.168.0.8*** then just take *MAC* Adress from *source field*

```
Frame 965: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: VMware_ce:5b:7b (00:0c:29:ce:5b:7b), Dst: VMware_d1:55:04
(00:0c:29:d1:55:04)
    Destination: VMware_d1:55:04 (00:0c:29:d1:55:04)
        Address: VMware_d1:55:04 (00:0c:29:d1:55:04)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: VMware_ce:5b:7b (00:0c:29:ce:5b:7b)
        Address: VMware_ce:5b:7b (00:0c:29:ce:5b:7b)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.8, Dst: 192.168.0.7
Internet Control Message Protocol
```

Answer is ***00:0C:29:CE:5B:7B***

Поисковые запросы

The condition of a given task:

Приведите пример поисковых запросов, использующих данные приемы:

- Точное совпадение
- Исключение слов
- Wildcard шаблоны (*)
- AROUND
- Related:
- Cache:

Solution:

i really tryna find out smth useful from task but it's kinda challenge for my patience my answer is **cache:www.youtube.com related:rutube.ru "MrBeast" -MrBro Страна AROUND(1) Земл***

Answer is ***cache:www.youtube.com related:rutube.ru "MrBeast" -MrBro Страна AROUND(1) Земл****

Политика обработки персональных данных

The condition of a given task:

Найдите политику ИТМО в отношении обработки персональных данных (в формате PDF). В качестве ответа приведите её md5sum

Solution:

the key link to pdf can found with request `filetype:pdf политику ИТМО в отношении обработки персональных данных` download it with wget: `wget https://itmo.ru/file/pages/79/personal_data_policy.pdf` and do `md5sum personal_data_policy.pdf`

Answer is ***87e5d25b5afdac4bb209b7be38ba5967***

Присмотритесь к сайту

The condition of a given task:

В ИТМО есть курс по OSINT (на ФБИТ). Попробуйте понять на этой основе и видя адрес текущего сайта с LMS2.0 платформой, на которой вы решаете задания, какой сайт у этого курса.
1. Присмотритесь к сайту курса, там первая часть флага вида (например, flag{123abc})
2. Найдите на GitHub организацию этого курса (кстати, он называется "Технологии добычи и анализа данных в киберпространстве"). Ответом является полный URL данной организации без указания протокола (например, github.com/codex-team/)
Соберите итоговый флаг путем конкатенации ответов: flag{123abc}github.com/codex-team/

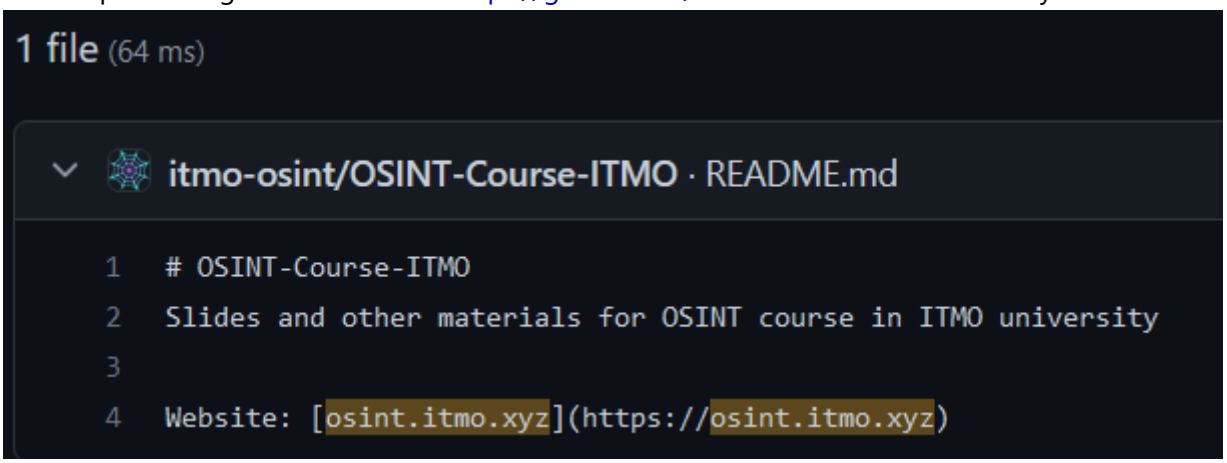
Solution:

the key host is osint.itmo.xyz inspect page source and take first part of flag

```
<html>
  <head></head>
  <body>
    Hello!
    <!--flag{cf9f0bcccfd3036c4a3c2993d34275b2}-->
  </body>
</html>
```

first part of flag is **flag{cf9f0bcccfd3036c4a3c2993d34275b2}**

second part of flag we can find with https://github.com/search with find osint.itmo.xyz in code



now we find out that company is github.com/itmo-osint

Second part of answer is **github.com/itmo-osint**

Answer is ***flag{cf9f0bcccfd3036c4a3c2993d34275b2}github.com/itmo-osint***

Старые хозяева

The condition of a given task:

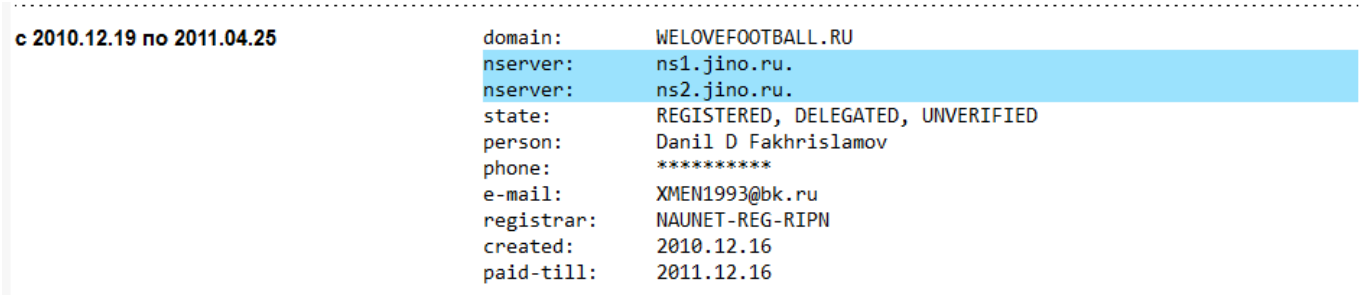
```
Найдите email и фамилию владельца домена welovefootball.ru Запишите ответ в нижнем регистре через запятую в виде: lower@case.ru,durov
```

Solution:

going to waybackmachine and search latest snapshot with https://web.archive.org/web/20160610071524/http://www.welovefootball.ru/about/ look smth like

Вас обслуживает ИП **Цырульников** М.Д. ИНН: 773012905652 ОГРНИП: 311774615700860 and this is ***fuckung dead end road***

just check on http://whoishistory.ru/ and see smth like



Answer is ***xmen1993@bk.ru,fakhrislamov***

DNS expiration

The condition of a given task:

⚠ Подключитесь к VPN сети
Вам доступен DNS сервер. Сколько часов держать значение в кэше до повторной проверки для домен expiration.osint
Подсказка
Например, вам был сгенерирован следующий IP: 10.10.10.10:49666. Это значит, что DNS сервер располагается на сервере с адресом 10.10.10.10 и слушает на порту 49666.

Solution:

just use ***DIG!*** in my case i need to write `dig @10.10.10.10 -p <my_port> expiration.osint` Answer from server is `;; communications error to 10.10.10.10#32844: timed out`
`; <<>> DiG 9.18.16-1-Debian <<>> @10.10.10.10 -p 32844 expiration.osint ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59531 ;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0 ;; WARNING: recursion requested but not available`
`;; QUESTION SECTION: ;expiration.osint. IN A`
`;; ANSWER SECTION: expiration.osint. 604800 IN A 1.1.1.1`
`;; Query time: 19 msec ;; SERVER: 10.10.10.10#32844(10.10.10.10) (UDP) ;; WHEN: Fri Sep 15 23:07:06 MSK 2023 ;; MSG SIZE rcvd: 66` QUERY is TTL in seconds, `604800/60/60 = 10080/60 = 168` hours

Answer is ***168***

DNS Resolve

The condition of a given task:

⚠ Подключитесь к VPN сети.
Вам доступен DNS сервер. Какой IP адрес резолвится по домену test.osint
Подсказка
Например, вам был сгенерирован следующий IP: 10.10.10.10:49666. Это значит, что DNS сервер располагается на сервере с адресом 10.10.10.10 и слушает на порту 49666.

Solution:

just use ***DIG!*** in my case i need to write `dig @10.10.10.10 -p <my_port> test.osint` Answer from server is `; <<>> DiG 9.18.16-1-Debian <<>> @10.10.10.10 -p 32841 test.osint ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15118 ;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0 ;; WARNING: recursion requested but not available ;; QUESTION SECTION: ;test.osint. IN A ;; ANSWER SECTION: test.osint. 3600 IN A **1.1.1.1** ;; Query time: 10 msec ;; SERVER: 10.10.10.10#32841(10.10.10.10) (UDP) ;; WHEN: Fri Sep 15 23:00:00 MSK 2023 ;; MSG SIZE rcvd: 54`

Answer is ***1.1.1.1***

Кто качал торрент

The condition of a given task:

`Найдите IP адрес и название игры, которую скачали 11 окт. 2023 г. около 8 часов утра с компьютера, IP адрес которого принадлежит университету ИТМО. Известно, что в этом адресе присутствует число 199. Ответ имеет формат IP адреса и названия на английском языке через запятую: "8.8.8.8,Warcraft". В названии нужно исключить версию игры, автора сборки и т.д. (в том числе без версии самой игры)`

Solution:

That is **sick** at first we need to check *ASN* of ITMO UNIVERSITY and i prefer use https://bgp.he.net/ just type *itmo* and check AS42289 where we can see the *Prefix v4* `77.234.199.0/24` next step is go to https://iknowwhatyoudownload.com/en/peer/?ip=77.234.199.0 now we can go to the near nodes, thanks God *iknowwhatyoudownload* can help us find their IPs like on pic below:

> Use internet connection of other people (Wi Fi, their computers, tablets and smartphones) to know what they download in torrent network, spy on them via special generated link or see other similar IPs: 77.234.199.3 **77.234.199.23** 77.234.199.27 77.234.199.29

we have now found out that 77.234.199.23 was distributing **Civilization** on the date and time specified in the assignment.

Answer is ***77.234.199.23,Civilization***

Угон домена

The condition of a given task:

`Сделайте так, чтобы ваш ИСУ ID отображался при переходе на домен, заканчивающийся на osinthijacking.itmo.xyz Пришлите ссылку на свой домен в виде ответа на задание`

Solution:

create index.html with content like

```
<html lang="en">
<head>
  <title>anythingbutit</title>
</head>
  <body>
  <p>311660</p>
  </body>
</html>
```

then create a file CNAME with your domain name only inside, in my case it *trashBu7int3r3st1ng.osinthijacking.itmo.xyz* and deploy with Github Pages link may help you `https://github.com/<Username_On_GitHub>/<Repository_Name>/settings/pages`

Answer is ***http://trashbu7int3r3st1ng.osinthijacking.itmo.xyz/***
