THM_S3BOTS2 [300 series questions]

Question 1

Mallory's critical PowerPoint presentation on her MacBook gets encrypted by ransomware on August 18. What is the name of this file after it was encrypted?

Frothly_marketing_campaign_Q317.pptx.crypt

clues: Mallory | PowerPoint | MacBook | August 18

index="botsv2" ".ppt"

results: 4 events; two on Aug 29 and two on Aug 24; what gives?

Let's start over

index="botsv2" Mallory

Account_Name: mallory.kraeusen

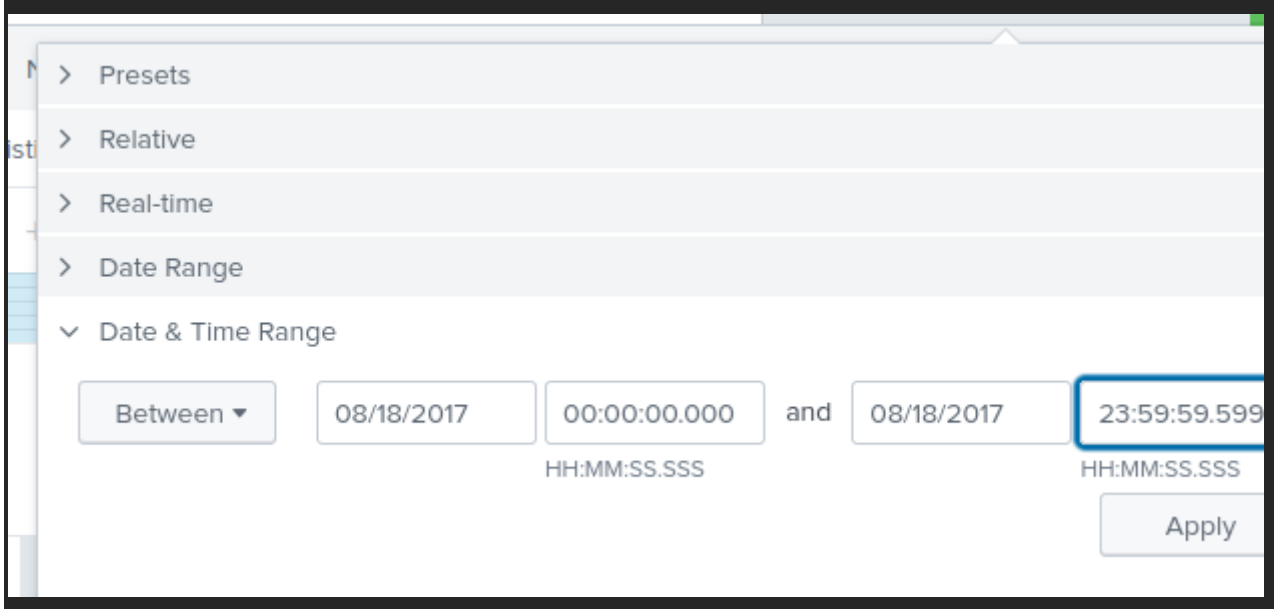
Account_Domain: FROTHLY

ComputerName: venus.frothly.local; mercury.frothly.local

Host: MACLORY-AIR13--a MacBook Air 13?

index="botsv2" MACLORY-AIR13

Looks like I can narrow this to Aug 18, 2017



Complete 1,412,821 events (8/18/17 12:00:00.000 AM to 8/18/17 11:59:59.599 PM)

What!? She uses her computer too much! Maybe getting it locked up will do her some good!!!!!

index="botsv2" MACLORY-AIR13 PowerPoint

Results: 0

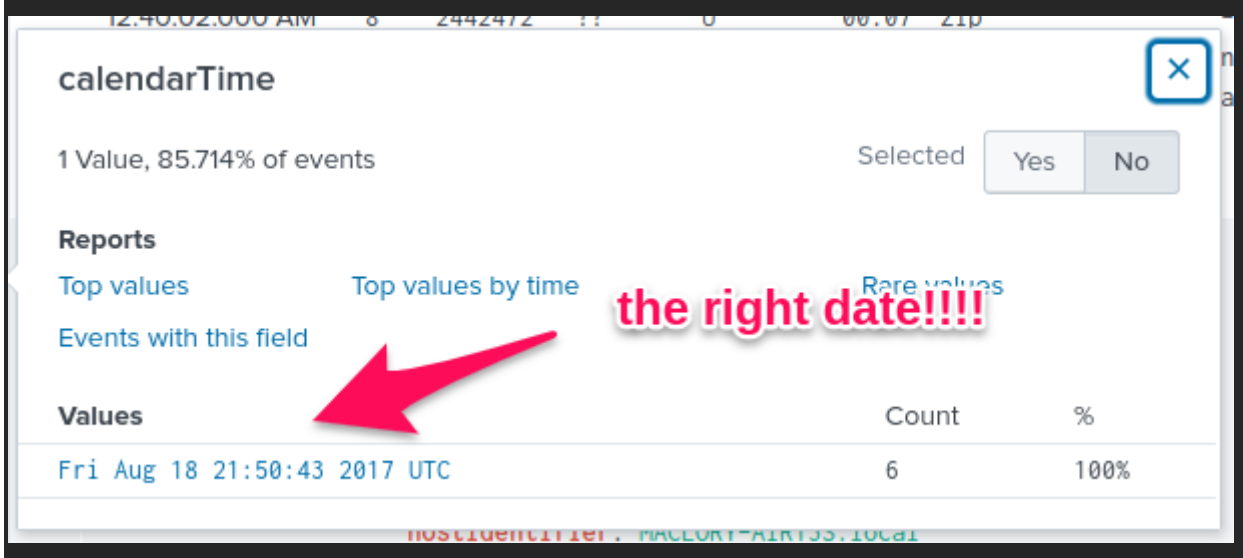
No Good

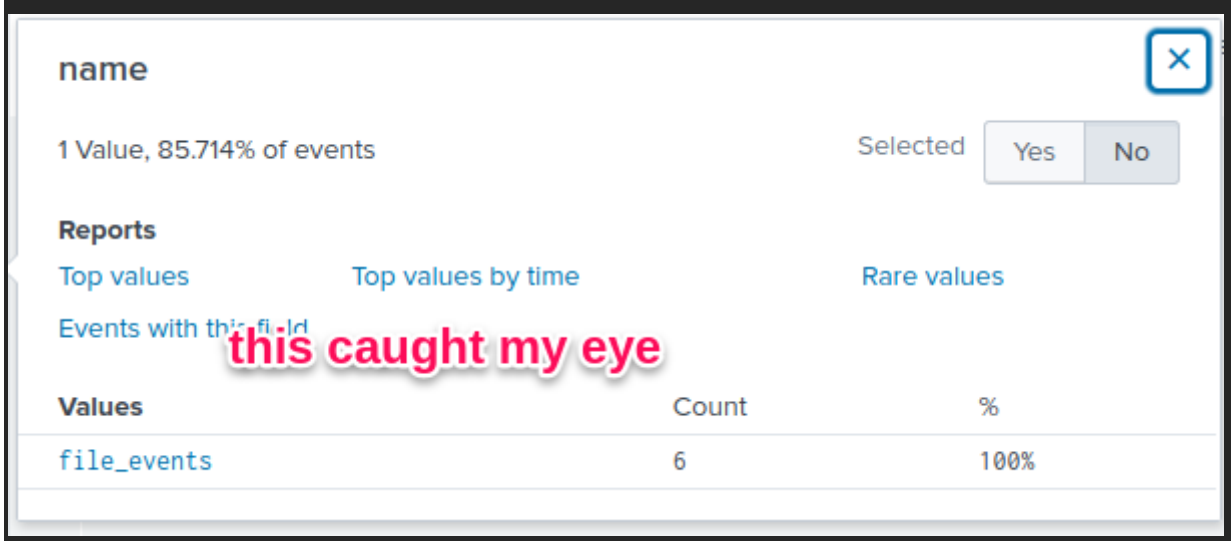
FROM THE GUIDE

index="botsv2" host="MACLORY-AIR13" (*.ppt OR *.pptx)

Maybe my time is should be "all time" since she didnt make the presentation on the 18th.

index="botsv2" host="MACLORY-AIR13" (*.ppt OR *.pptx)





But if I had just looked at the main field I would have seen this right in front my face

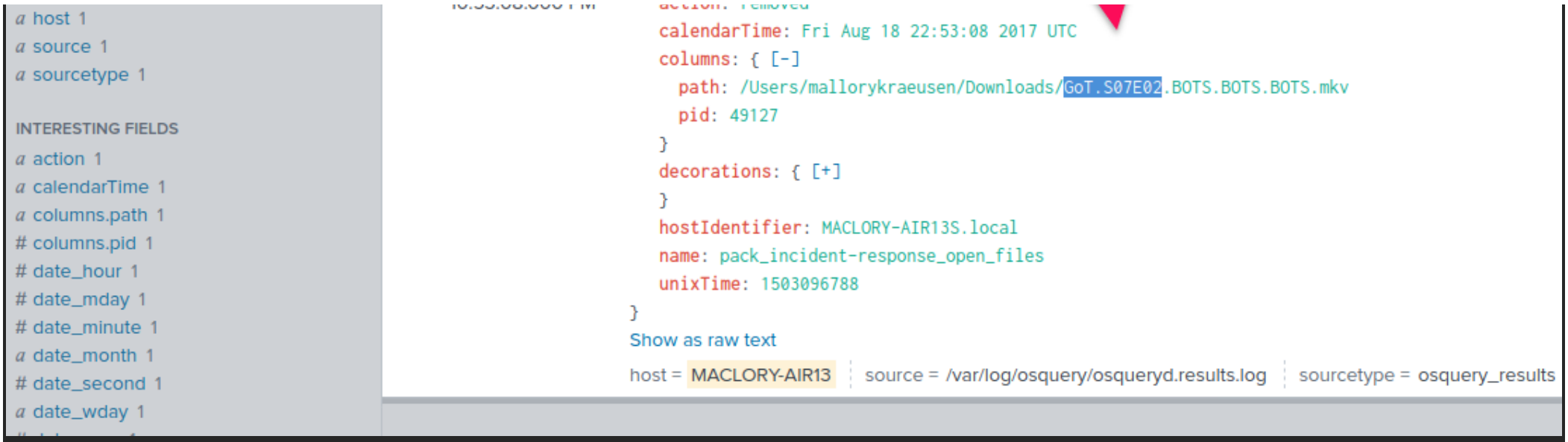
Question 2

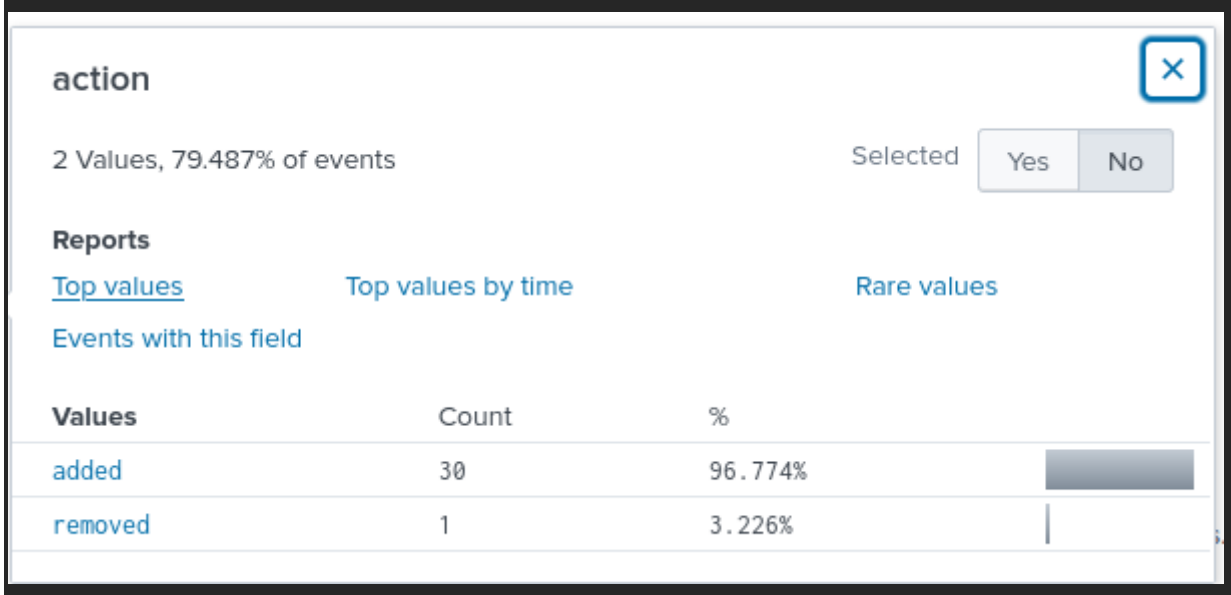
There is a Games of Thrones movie file that was encrypted as well. What season and episode is it?

Season 07; Episode 02

Let me try this:

index="botsv2" host="MACLORY-AIR13" ("GoT" OR "Game of Thrones")





index="botsv2" "kutekitten""\\/Users"

Question 3
Kevin Lagerfield used a USB drive to move malware onto kutekitten, Mallory's personal MacBook. She ran the malware, which obfuscates itself during execution. Provide the vendor name of the USB drive Kevin likely used. Answer Guidance: Use time correlation to identify the USB drive.
Alcor Micro Corp.--WHAT A BITCH OF A QUESTION!!!! This took me nearly an hour to answer.

index="botsv2" "kutekitten""\\/Users"
Plan: I need a list of all USBs connected to kutekitten; this can be xrefrenced with the time of infection or if I can figure out Kevin's machine, maybe I can find a USB record that matches one with Mal's
USB have a "MAC" address or something?

> **A USB pen drive doesn't have a MAC address**. MAC addresses are used for network devices while a pen drive is a storage device. However, many pen drives do have a serial number, which may or may not be unique.

```
sourcetype=winregistry friendlyname
```

> Expand a result and look at the registry_value_data field

I forgot about that^^^^^

Nope DEADEND

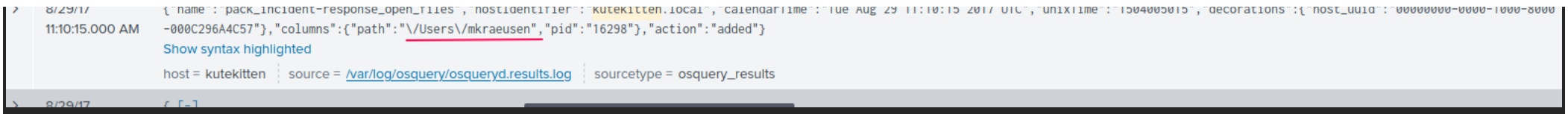
> **The number of returned events is over 6,000, and the 2 data sources/source types are related to Osquery.**
>
> **What is Osquery?**
>
> **"*Osquery exposes an operating system as a high-performance relational database. This allows you to write SQL queries to explore operating system data. With Osquery, SQL tables represent abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.*"**

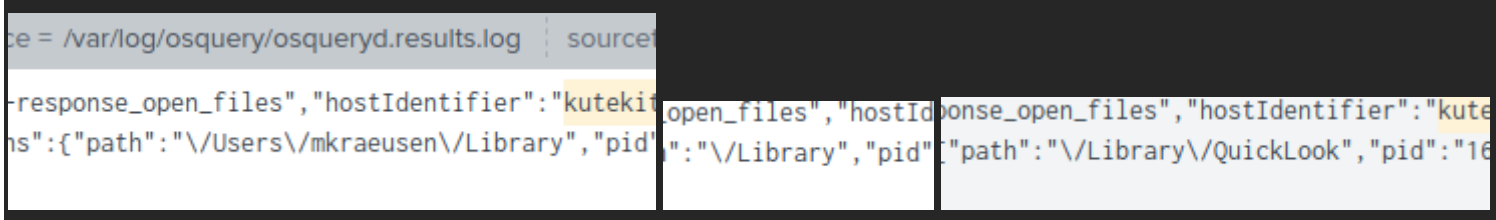
index="botsv2" "kutekitten""\\/Users"

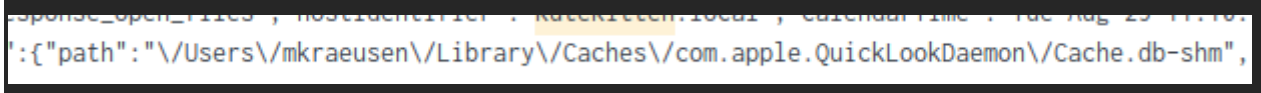
Apparently host="kutekitten" and just "kutekitten" return wildly different results and the more generic term gives fewer....curious

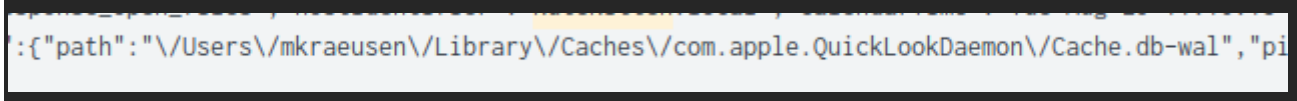
index="botsv2" "kutekitten"

The guide talks about looking in Mal's user folder eg "\\/***PATH***\\/***MALLORY***||/***FOLDER***"
I can find the path by looking at the raw text of some of these entries



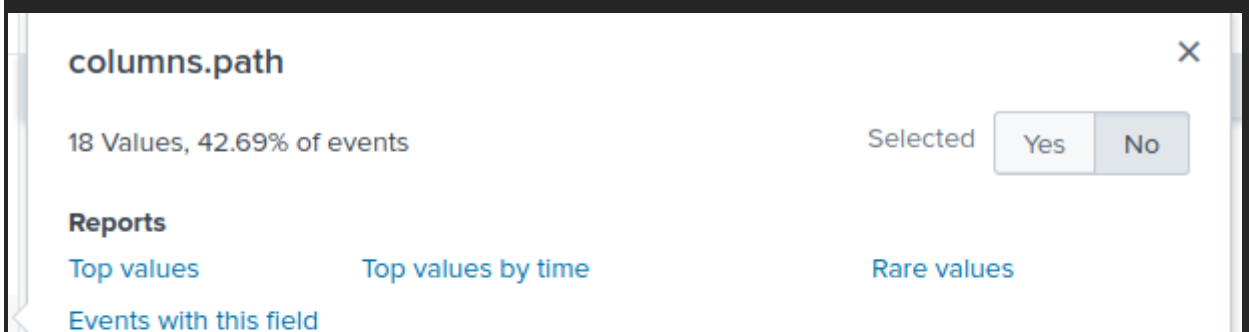




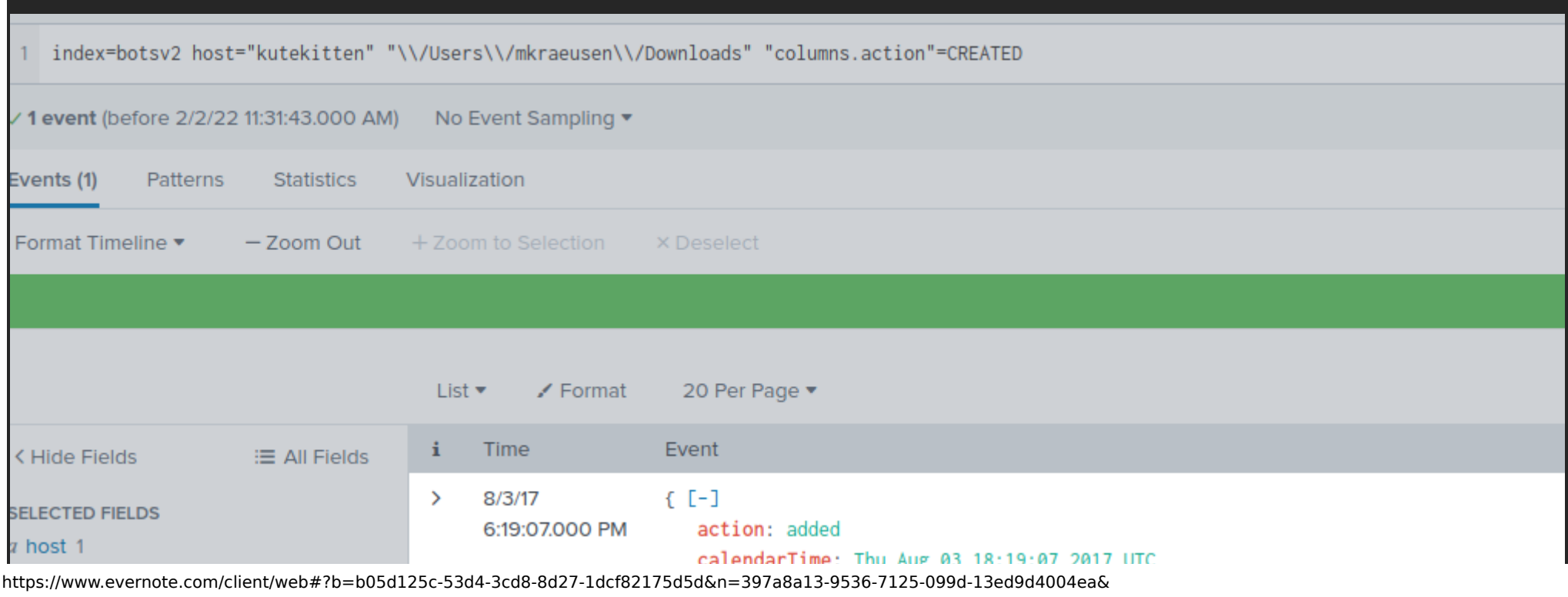


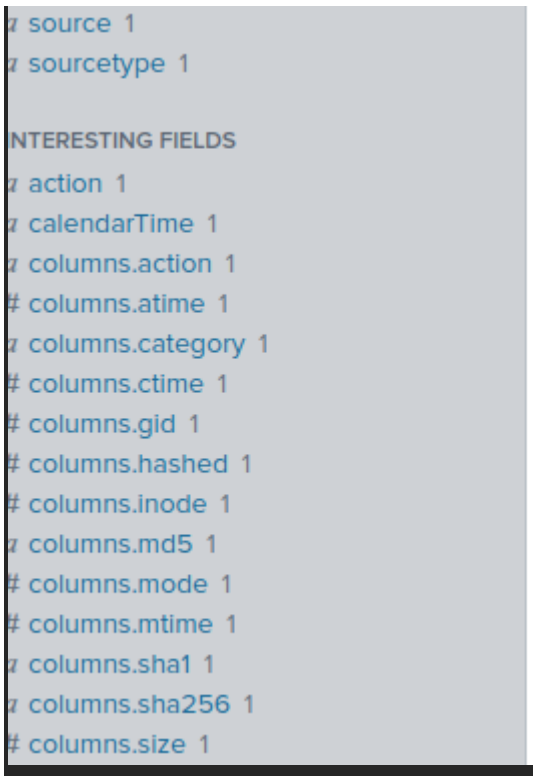
Looks like MANUAL ENUMERATION

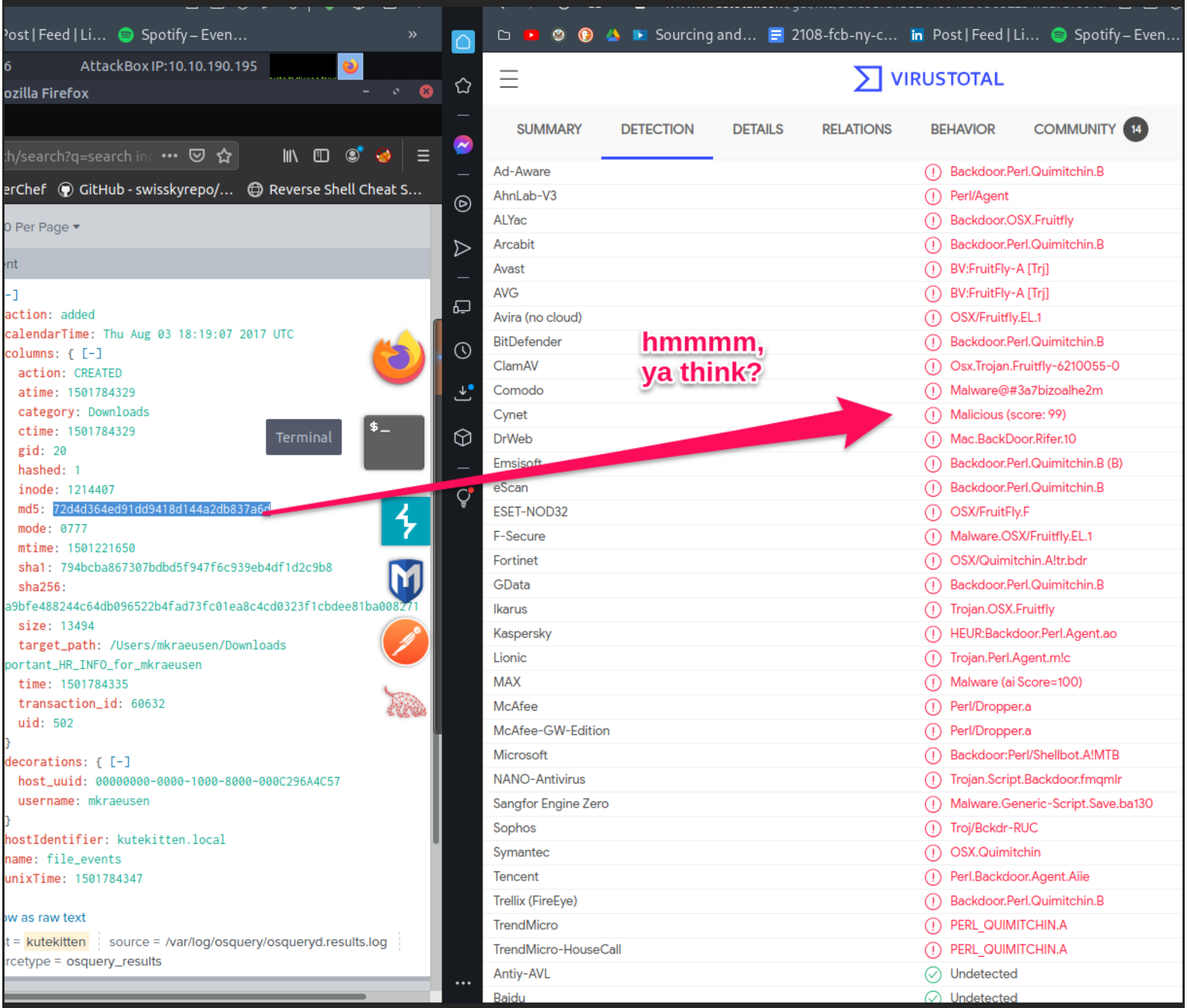
index="botsv2" "kutekitten""\\/Users"



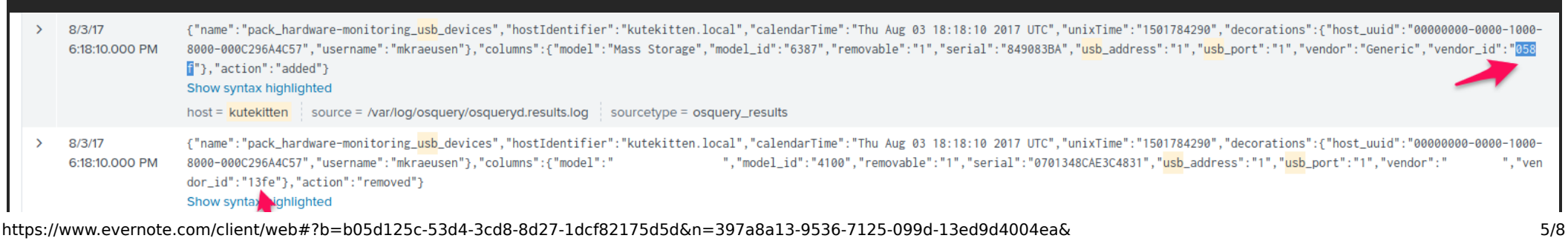
After Looking at the guide to point me to downloads (don't know how they figured that out) ; I jumped to action, created

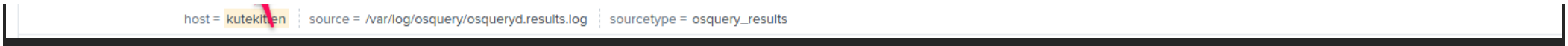






index=botsv2 host="kutekitten" USB





My Question

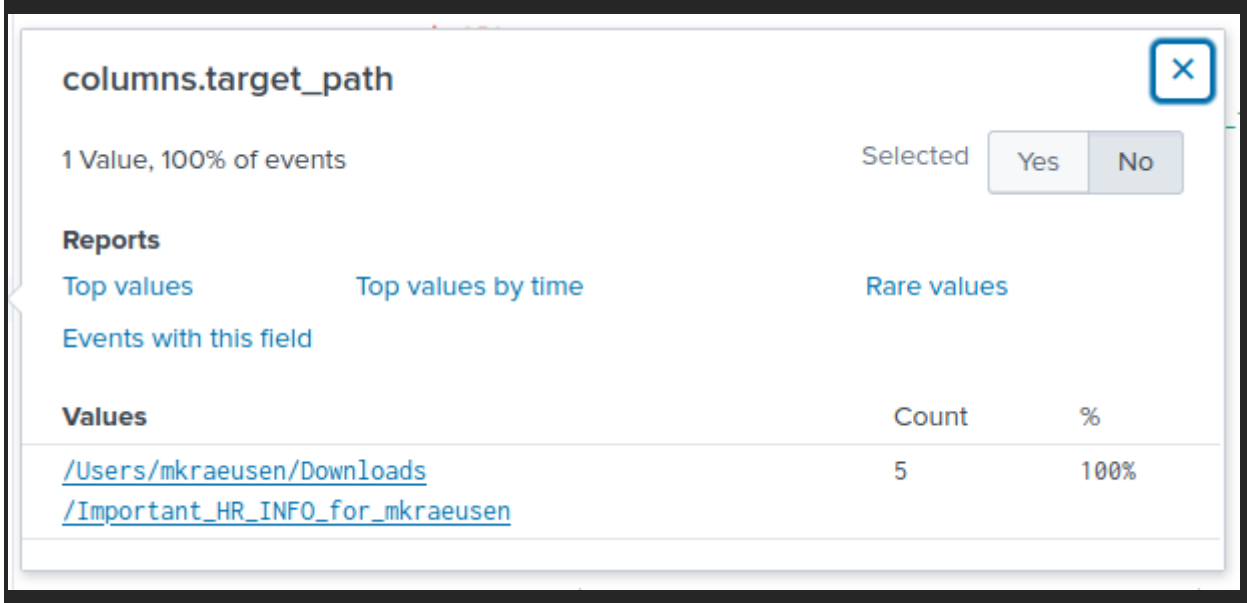
Why is there two different USB devices at the same time? Both were inserted(?) at the same time, just before the malware was installed? One belongs to Kingston, the other Alcor.

Question 4

What programming language is at least part of the malware from the question above written in?

Perl

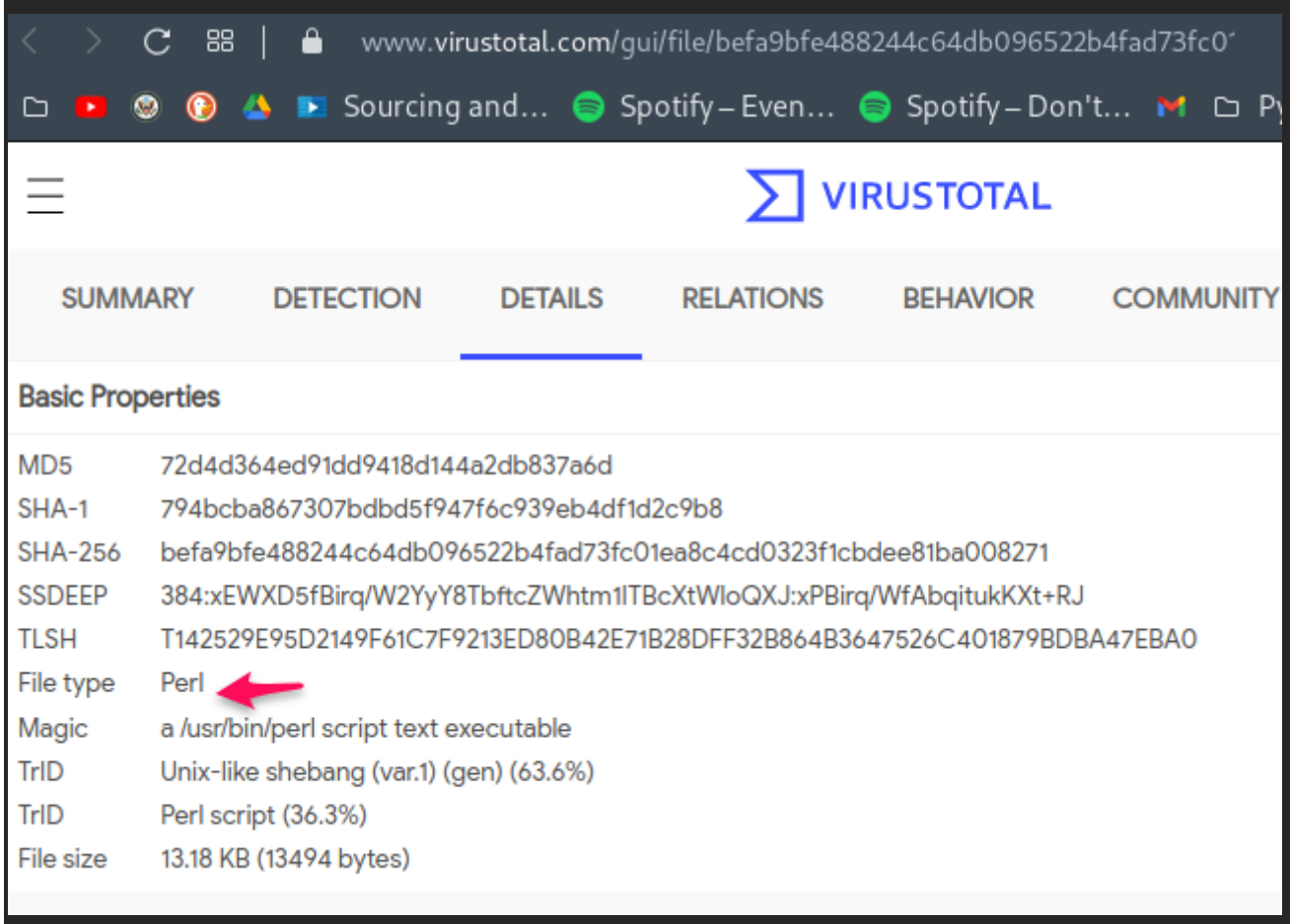
index="botsv2" "kutekitten""\\/Users\\/mkraeusen\\/Downloads"
Brings us to:



index="botsv2" "kutekitten""\\/Users\\/mkraeusen\\/Downloads"
"columns.target_path"="/Users/mkraeusen/Downloads/Important_HR_INFO_for_mkraeusen"

This brings up 5 entries but all I know is to look at the raw text for something, but I see nothing that points me to the answer.

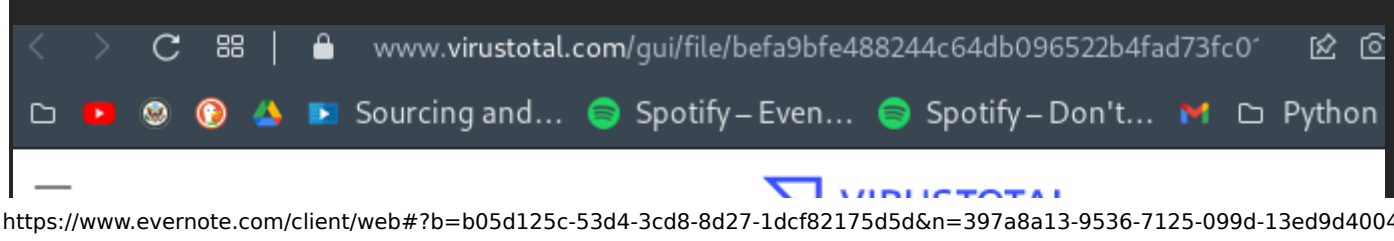
Ah, it was back on the virustotal entry under details

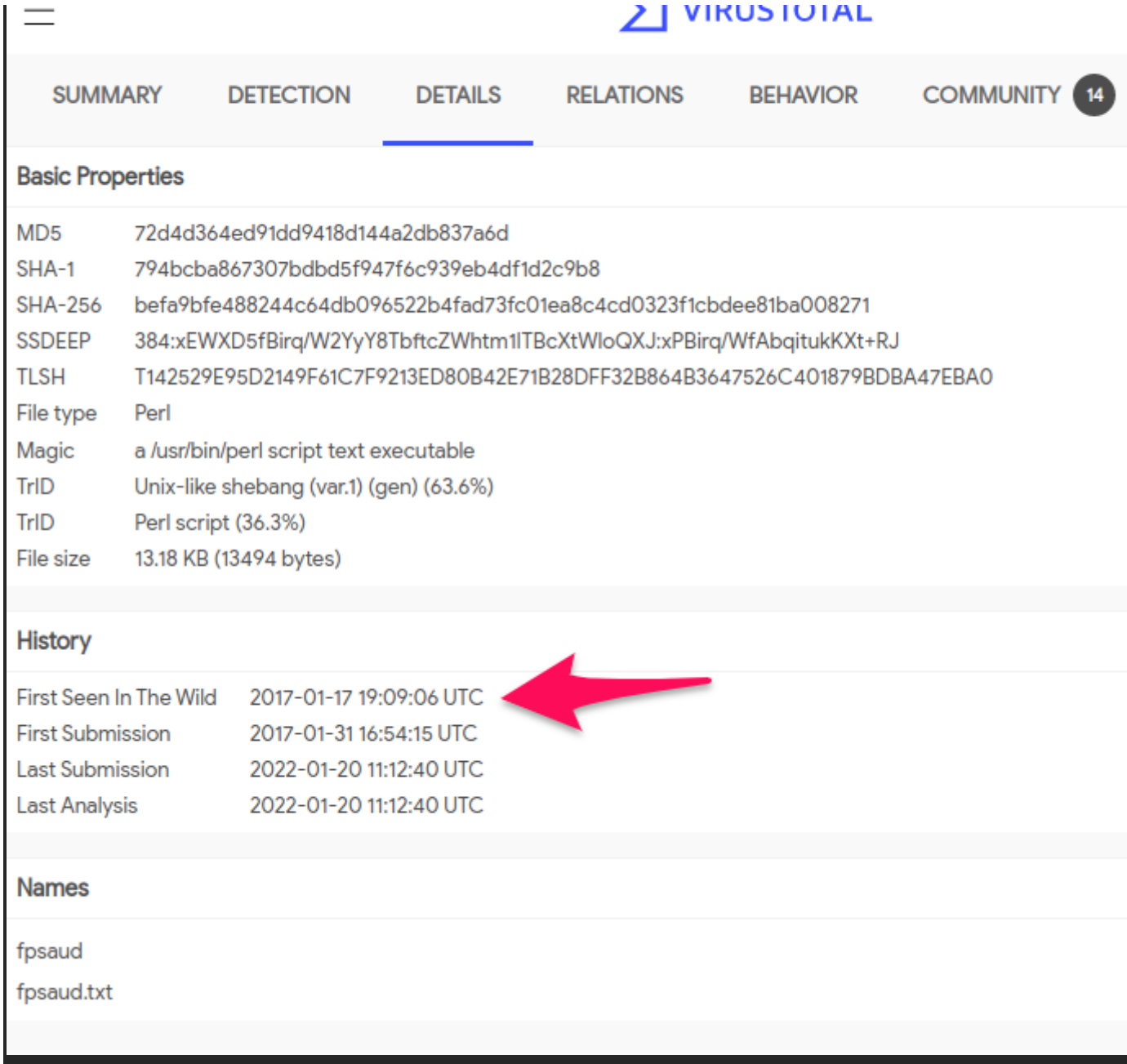


Question 5

When was this malware first seen in the wild? Answer Guidance: YYYY-MM-DD

2017-01-17

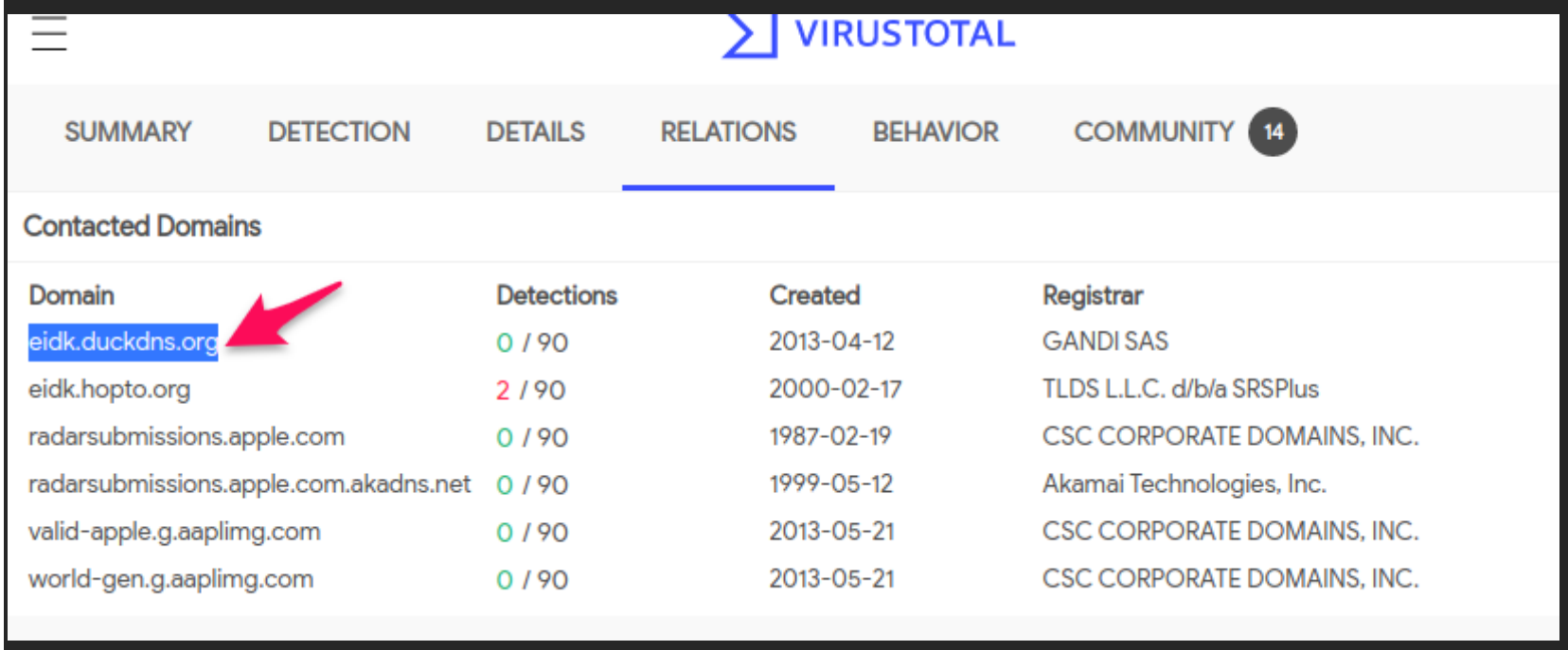




Question 6

The malware infecting kutekitten uses dynamic DNSdestinations to communicate with two C&C servers shortly after installation. What is the fully-qualified domain name (FQDN) of the first (alphabetically) of these destinations?

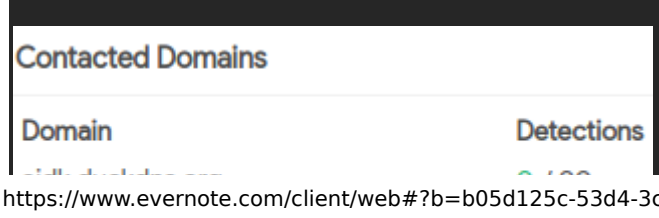
eidk.duckdns.org

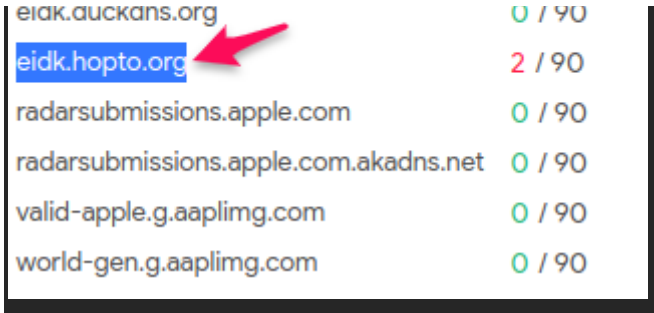


Question 7

From the question above, what is the fully-qualified domain name (FQDN) of the second (alphabetically) contacted C&C server?

eidk.hopto.org





I guess these last 4 questions were to make up for the pain of question 3