

## Lab 1

### Task 1 : Gather Information

#### Passive recon

#### 1. Introduction

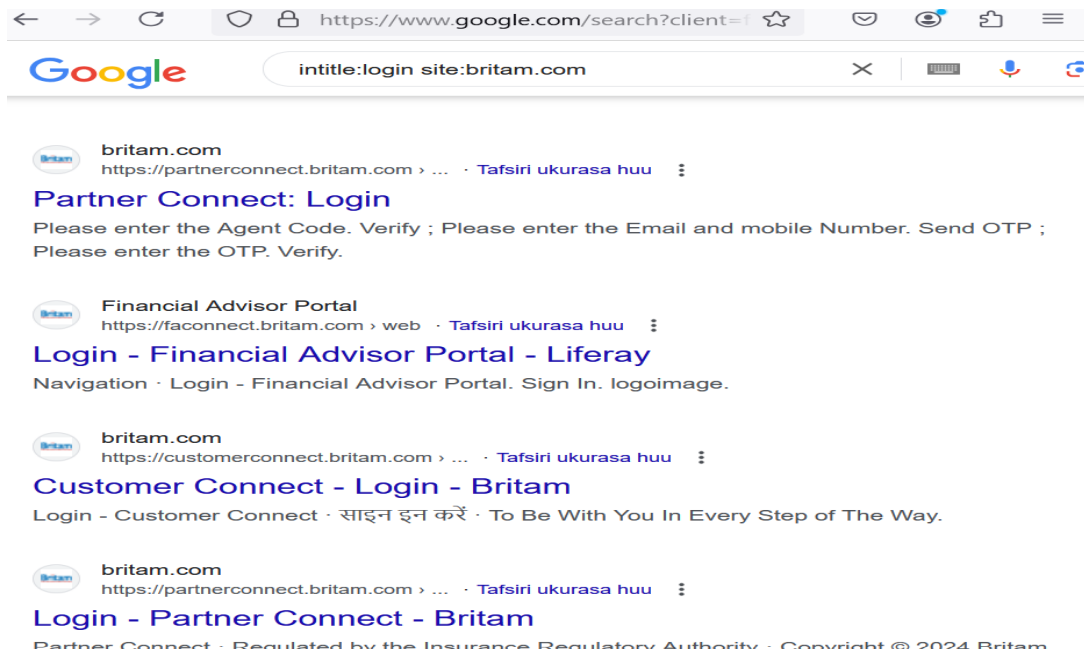
- **Objective:** The goal of this task was to gather publicly available information about the target organization (Britam) using advanced Google search operators. The focus was on identifying potential login pages and retrieving documents in PDF format that could contain useful metadata or sensitive information about the organization.
- **Target Organization:** Britam.

#### 2. Methodology

##### 2.1 Search for Login Pages Using Google Advanced Operators

- **Search Query:** We used the query **intitle:login site:britam.com** to restrict the search results to pages on Britam's website containing the word "login" in the title.
- **Search Results:** The results included several login pages hosted on Britam's domain. Some key findings:
  - **customerconnect.britam.com/login:** Likely a portal for customer interactions or services.
  - **www.britam.com/login:** Likely the main corporate login page for internal access.

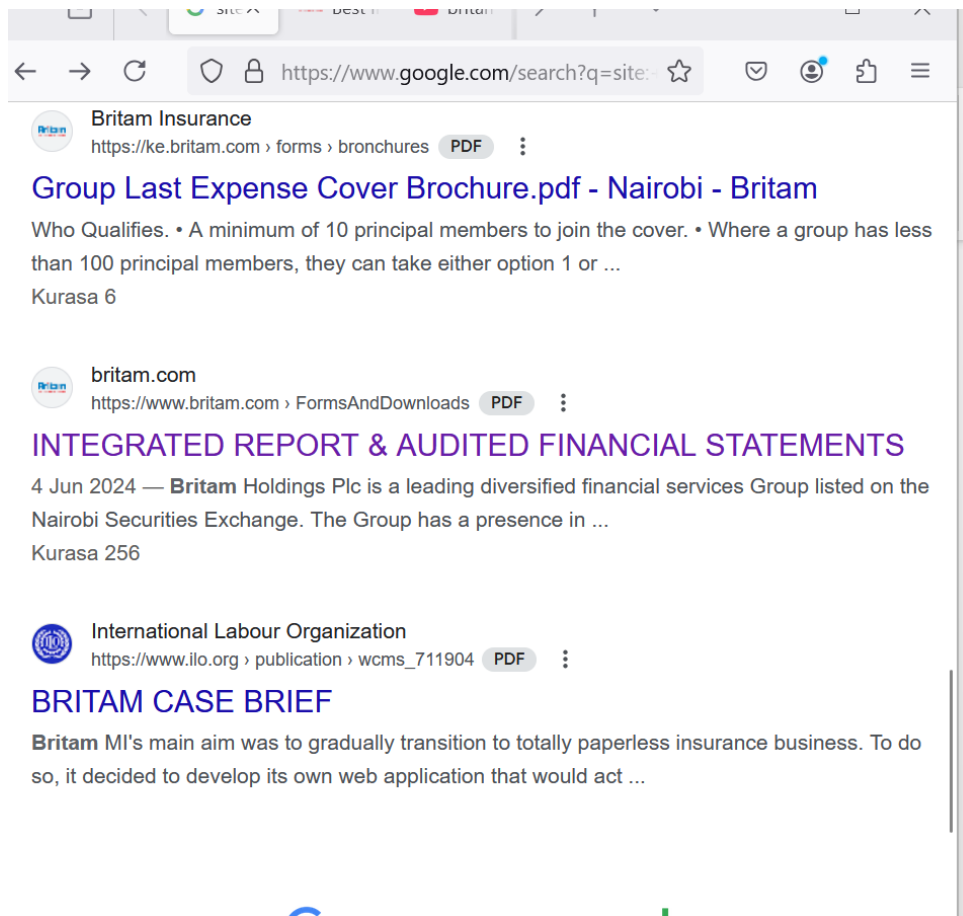
Figure 1 image of results of searching for login pages



## 2.2 Search for PDF Files Using Google Advanced Operators





- **Search Query:** We used the query filetype:pdf site:britam.com to find publicly accessible PDF documents on Britam's website.
- **Search Results:** The results included several PDF documents hosted on the Britam domain. Key findings:
  - **Company Brochures:** PDFs detailing the company's financial products and services.
  - **Annual Reports:** Documents containing detailed information about Britam's operations, financial performance, and strategic goals.

Figure 2 result of searching pdf files related to britam



**PDF Documents:**

- We accessed the **Annual Financial Report**, which included sensitive details such as:
  - **List of Directors:** Names and titles.
  - **Remuneration Details:** Salaries, bonuses, and benefits.
- **Exploitation Risk:** This information could be used for **social engineering attacks**, such as:
  - Crafting targeted phishing emails to directors based on their roles and salaries.

60 of 256   —   +   Automatic Zoom            

Board Member	Position	Annual Retainer	Sitting Allowance	Other Allowances	Salaries and Other Benefits	Total
Mr. Kuria Muchiru	Chairman	1,000,000	1,775,000	10,240,000	-	13,015,000
Dr. Peter K. Munga	NED	1,000,000	1,900,000	-	-	2,900,000
Mr. Jimnah M. Mbaru	NED	1,000,000	1,487,500	-	-	2,487,500
Mrs. Caroline Kigen	NED	1,000,000	1,487,500	-	-	2,487,500
Africinvest III SPV- Represented by Mr. George Odo	NED	1,000,000	2,500,000	-	-	3,500,000
Mr. Edouard Shomid	NED	-	-	-	-	-
Ms. Josephine Ossiya	NED	250,000	162,500	-	-	412,500
Mr. Julius Mbayi	INED	1,000,000	3,462,500	-	-	4,462,500
Ms. Celestine Munda	INED	1,000,000	2,725,000	-	-	3,725,000
Mr. Tom Gitogo	ED	-	-	-	93,818,550	93,818,550
Mr. Lotfi Baccouche	INED	1,000,000	1,975,000	-	-	2,975,000
Ms. Susan Abisola	NED	750,000	1,375,000	-	-	2,125,000
Ms. Barbara Chesire (Co-opted CXI Committee Member)	NED	-	250,000	-	-	250,000
<b>Total</b>		<b>9,000,000</b>	<b>19,100,000</b>	<b>10,240,000</b>	<b>93,818,550</b>	<b>132,158,550</b>

NED - Non-executive Directors  
INED - Independent Non-executive Directors

## Task 2 Gather Information from Video Search Engines

### 1.Introduction

- **Objective:** The goal of this task was to gather information about the target organization (Britam) by using advanced video search and reverse image search techniques. This helped in identifying publicly available metadata from YouTube and performing a reverse image search to gather additional insights.
- **Target Organization: Britam.**

### 2. Methodology

#### 2.1 Searching for the Organization on YouTube

- **Search Query:** we searched for videos related to **Britam** on YouTube using the search term Britam.
- **Search Results:** we examined the list of videos related to Britam that appeared in the search results. Some of the videos included:

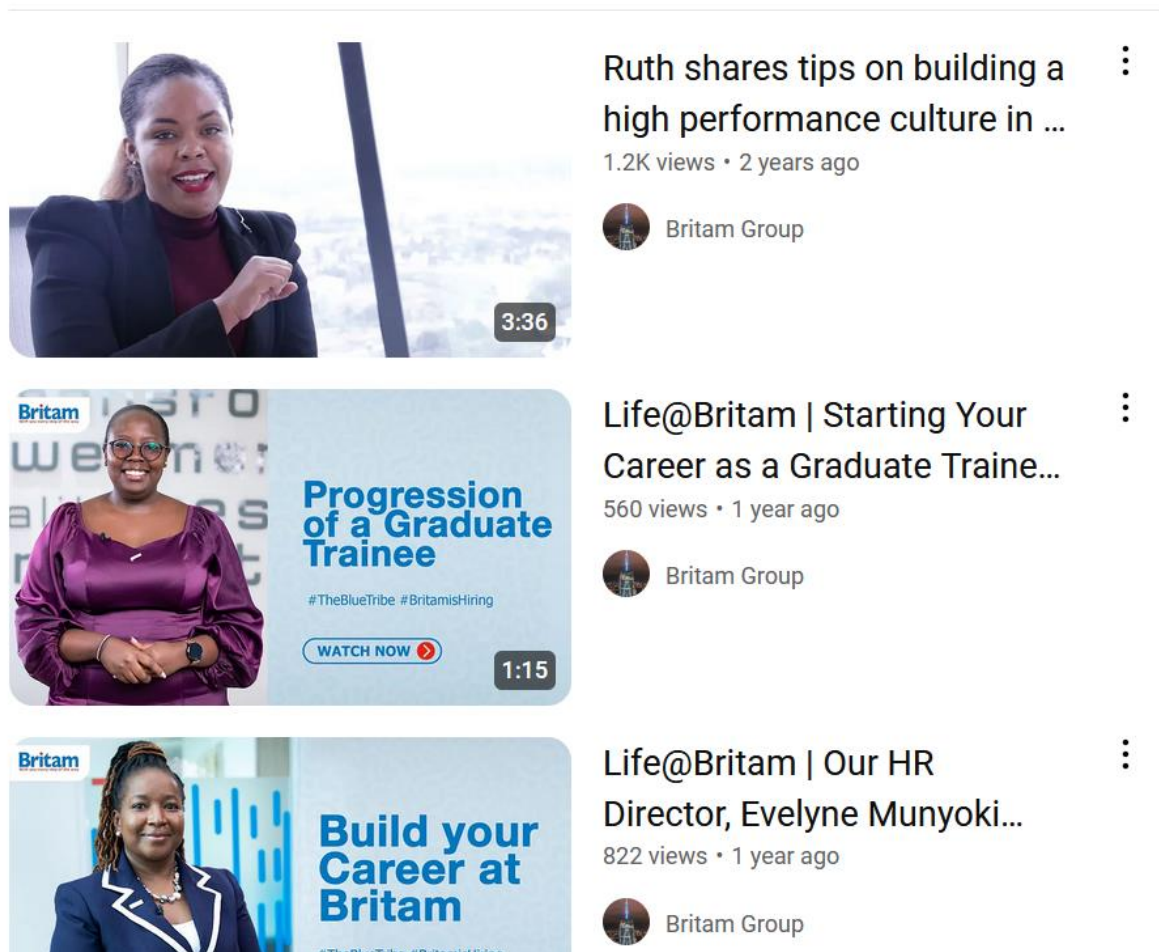


Figure 3 image of results from video search of britam

## 2.2 Video Metadata Extraction

- **Tool Used:** we used the YouTube Metadata tool (found at [mattw.io/youtube-metadata](https://mattw.io/youtube-metadata)) to gather metadata details for the selected videos.
- **Video URL:** The URL of the video we selected is <https://www.youtube.com/watch?v=DPJVvZ-HfGw&pp=ygUGYnJpdGFt>
- **Metadata Gathered:**

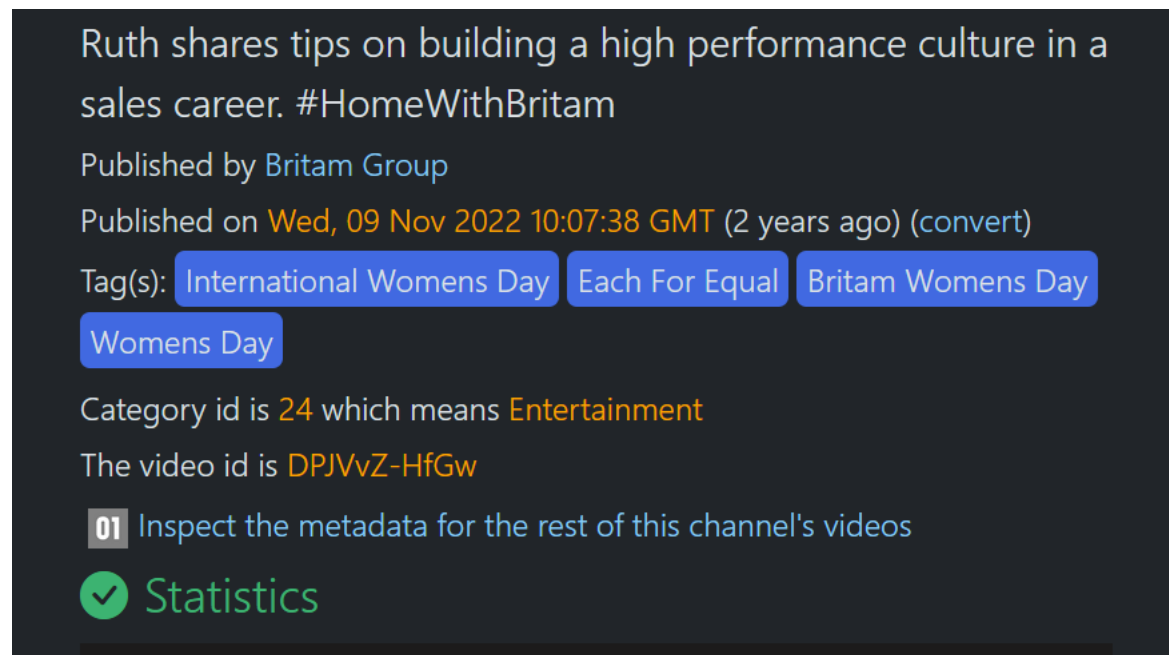
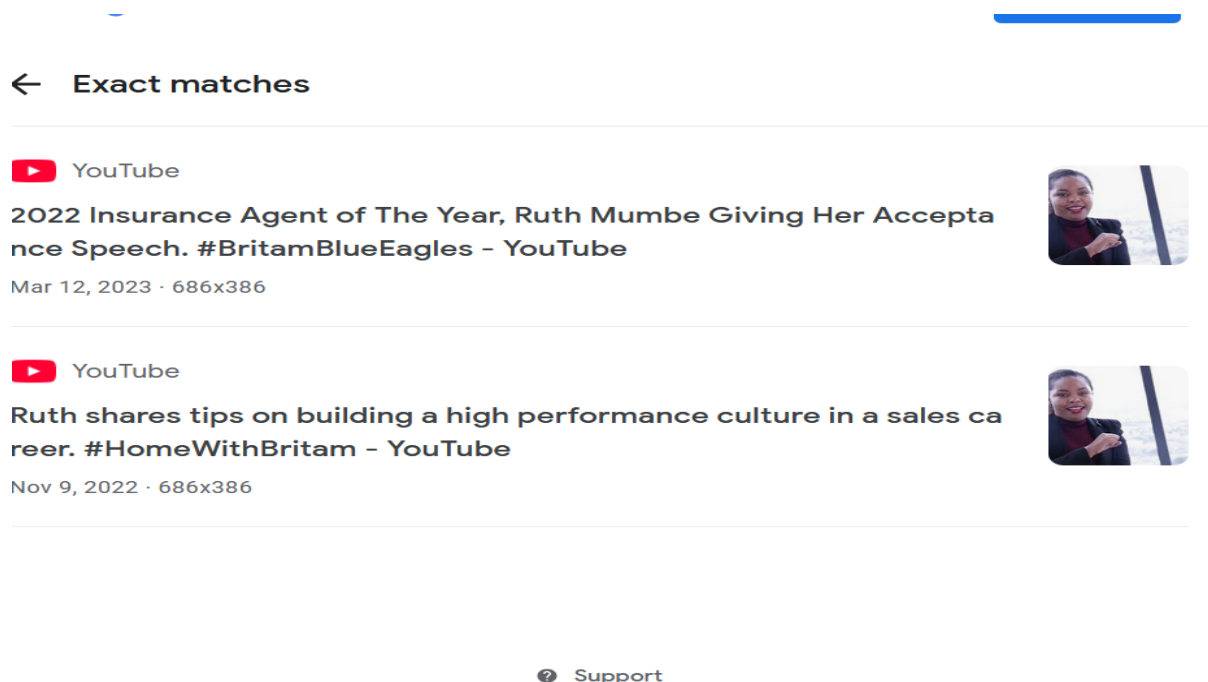


Figure 4 image of results of the video metadata

## 2.3 Reverse Image Search

- **Reverse Image Search:** we used the reverse image search feature in the YouTube Metadata tool to analyse the video thumbnail.
- **Reverse Image Search Result:** By using Google's reverse image search, we found that the thumbnail was used in:

Figure 5 results of the thumbnail reverse image search



## 3. Findings

### 3.1 Insights from Metadata

- The metadata provided valuable information regarding the video's creator, upload date, and associated tags.
  - **Video 1:** <https://www.youtube.com/watch?v=DPJVVZ-HfGw&pp=ygUGYnJpdGFt>
    - **Published on:** Wed, 09 Nov 2022 10:07:38 GMT
    - **Uploader:** Britam group channel
    - **Geolocation:** the Britam group channel was created in Nairobi Kenya.

### 3.2 Insights from Reverse Image Search

- The reverse image search revealed additional websites where the video thumbnail appeared, giving further context to the video.
- we were able to identify the name of the media executive since another video uploaded on YouTube had the name, this can potentially be used for social engineering attack.

## Task 3: Gather Information from FTP Search Engines

### 1. Introduction

- **Objective:** To explore publicly accessible FTP servers using FTP search engines and gather potential information about Britam.

### 2. Methodology

- **Tool Used:**
  - NAPALM FTP Indexer (<https://www.searchftps.net/>).
- **Steps Taken:**
  - Accessed the FTP search engine via Mozilla Firefox.
  - Typed "**Britam**" as the search query.

### 3. Findings

- The search query returned **no results** related to Britam.



## Task 4 Gather Information from IoT Search Engines

### 1.Shodan Search Results:

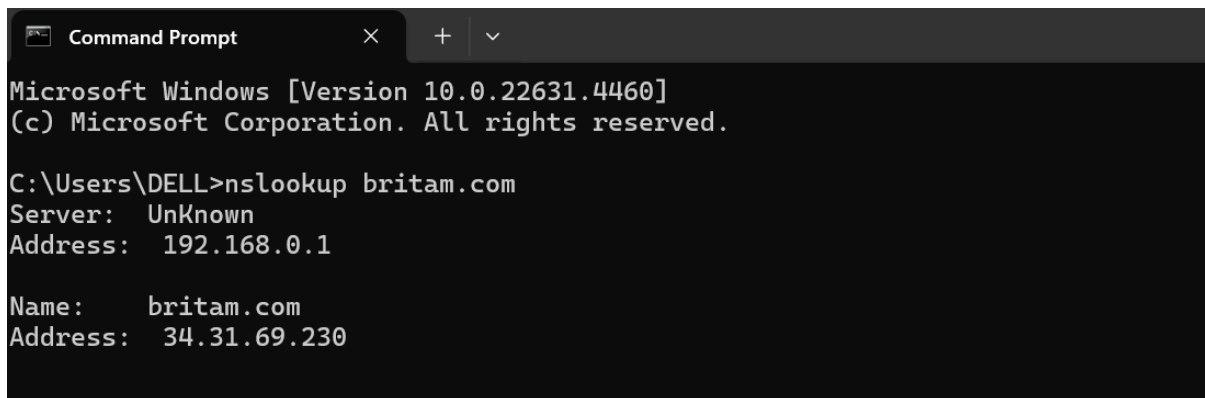
A search for Britam on Shodan revealed no immediate vulnerabilities.

### 2. NSLookup for IP Address:

- **Command Used:** nslookup britam.com
- **IP Address:** 34.32.69.230

**Findings:** By performing an **NSLookup** query, we successfully retrieved the public IP address of Britam's domain (**34.32.69.230**). This confirms that Britam's website and services are hosted at this IP address, and it is essential for further analysis using IP-based tools such as **Censys**.

Figure 6 image of cmd used for nslookup



```
Command Prompt
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>nslookup britam.com
Server: UnKnown
Address: 192.168.0.1

Name:    britam.com
Address: 34.31.69.230
```

### 3. Censys Analysis:

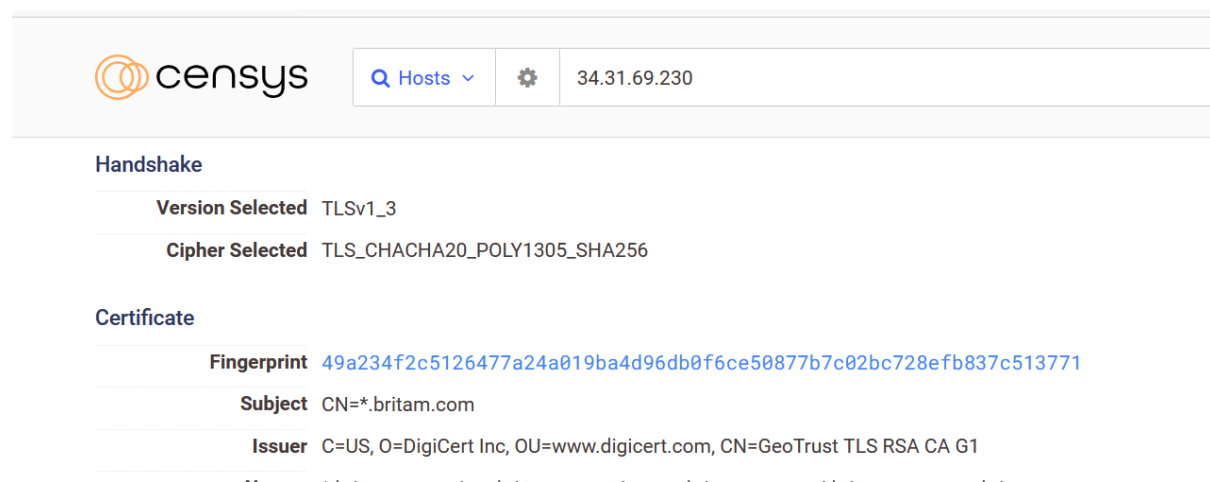
Using **Censys** for deeper analysis of the IP address **34.32.69.230**, the following details were gathered:

- **TLS Protocol Version:** TLSv1.3
- **Cipher Suite:** TLS\_CHACHA20\_POLY1305\_SHA256
- **Certificate Fingerprint:**  
49a234f2c5126477a24a019ba4d96db0f6ce50877b7c02bc728efb837c513771
- **Subject (CN):** \*.britam.com (Wildcard certificate)
- **Issuer:** DigiCert Inc, GeoTrust TLS RSA CA G1

### Findings:

- **Strong Encryption:** The server uses **TLSv1.3** a highly secure encryption method resistant to modern attacks.

Figure 7 img of results of the ip search using cenys



### Conclusion:

Based on the information gathered, Britam is using strong encryption protocols (TLSv1.3) and a trusted certificate authority (DigiCert). While the **Shodan** search did not yield results, using **NSLookup** and **Censys** provided the public IP address and further detailed inspection. The IP address **34.32.69.230** is associated with Britam's infrastructure, and no immediate vulnerabilities were identified from the TLS certificate inspection.

# LAB 2


## TASK 1 find the companyis domain and subdomain using netcraft

### 1. Introduction

This report outlines the findings from the investigation of the domain britam.com and its associated subdomains. The investigation was conducted to identify potential points of attack and assess the surface area for cybersecurity risks.

### Domain and Subdomain Information:

- **Domain Name:** britam.com
- **Subdomains Identified:**
  - customerconnect.britam.com
  - ke.britam.com
  - [www.britam.com](http://www.britam.com)




LEARN MOREREPORT FRAUD

3 results

Rank	Site	First seen	Netblock	OS	Site Report
184989	<a href="http://customerconnect.britam.com">customerconnect.britam.com</a>	July 2017	Oracle Corporation	unknown	
234289	<a href="http://ke.britam.com">ke.britam.com</a>	January 2020	Google LLC	unknown	
990555	<a href="http://www.britam.com">www.britam.com</a>	September 1996	Google LLC	unknown	

https://www.netcraft.com

Can't find what you're looking for?






LEARN MOREREPORT FRAUD

Background

Site title	Not Present	Date first seen	February 2020
Site rank	234010	Primary language	English
Description	Not Present		

Network

Site	<a href="https://ke.britam.com">https://ke.britam.com</a>	Domain	<a href="http://britam.com">britam.com</a>
Netblock Owner	Google LLC	Nameserver	ns-cloud-c1.googledomains.com
Hosting company	Google Cloud - Iowa datacenter	Domain registrar	Unknown
Hosting country	 us	Nameserver organisation	Unknown
IPv4 address	34.31.69.230 	Organisation	Unknown
IPv4 autonomous systems	AS396982 	DNS admin	cloud-dns-hostmaster@google.com

TASK 2 gather personal information using peekyou online

1. Introduction

This report outlines the findings from the use of **Peek You** to gather publicly available personal information about an individual. The investigation was performed to identify the extent of the individual's digital footprint and potential privacy concerns based on public data. The information was collected using publicly accessible online sources and does not include any non-public or private data.

2. Subject Information

- **Full Name:** James wambugu

Phonebook

Paid service sponsored by 2 partners

We Found James Wambugu

1) James Wambugu's Phone & Current Address

Search Details

2) Social Media Profiles & More

Search Details

James Wambugu's Phone #, Address & More

Search Details

James Wambugu's Contact Info, Social Profiles & More

Search Details

Email Addresses

Paid service sponsored by BeenVerified

View James's Profiles on Facebook and 60+ Networks, james\*\*\*\*@gmail

View James's Profiles on Facebook and 60+ Networks, james\*\*\*\*@yahoo

View James's Profiles on Facebook and 60+ Networks, james\*\*\*\*@hotmail

View James's Profiles on Facebook and 60+ Networks, james\*\*\*\*@aol

View James's Profiles on Facebook and 60+ Networks, james\*\*\*\*@outlook

Contact Information & Address History

Paid service sponsored by BeenVerified

James W...

Search address history, phone, age and more.

SEARCH DETAILS

James Wambugu

We found 1 records for James Wambugu

Public Records

Facebook

Instagram

Phonebook

Email Addresses

Page Overview:

Search results for James Wambugu reveal multiple individuals. Social media activity includes 15 Facebook, 5 Instagram, 18 Twitter, and 9 MySpace profiles, as well as 10 Wikipedia and 10 Flickr profiles. Public records list James S Wambugu, residing in Methuen, MA; James W Wambugu and James W Wambugu Njukia, both residing in Houston, TX; James D Wambugu, residing in Annapolis, MD; and James M W, James K W, James M w, and James S W, with no addresses listed. Additional individuals, James S Wambugu (age 40), James M Wambugu (age 46), and several others with the name James Wambugu, also appear without addresses. Web results indicate James Wambugu's involvement with the East African Banking Forum, Britam General Insurance Company Limited, and Uap Insurance Kenya Ltd, holding positions such as Managing Director. Other results highlight James Wambugu's roles as a Software Engineer, a qualified lawyer with a Masters Degree in Development Finance, and a Chairman. Various educational backgrounds are also mentioned, including MBA (Finance), Bcomm (Accounting), a Diploma in Risk Management, a Bachelor of Arts in Christian Education, and Law & BComm (Economics) degrees.

Each profile offers unique details, so explore the page for more information on each person.

Found in regions:

Georgia

James Wambugu

Atlanta, GA

By continuing to use our site, you consent to the placement of cookies on your browser and agree to the terms of our Privacy Policy. [More details](#)

I agree

James Wambugu from East African britam forum was found in the page overview

Ilya otaga

### TASK 3

No emails, hosts or Ips were found using theHarvester.

```
root@kali: /home/capsersudo
(capsersudo@kali) - [~]
$ sudo su
[sudo] password for capsersudo:
(root@kali) - [/home/capsersudo]
# theHarvester -d britam.com -l 200 -b baidu
Created default proxies.yaml at /root/.theHarvester/proxies.yaml
*****
*                                     *
* [theHarvester]                     *
* [theHarvester]                     *
* [theHarvester]                     *
* [theHarvester]                     *
* [theHarvester]                     *
* theHarvester 4.6.0                  *
* Coded by Christian Martorella       *
* Edge-Security Research              *
* cmartorella@edge-security.com       *
*                                     *
*****

[*] Target: britam.com
[*] Searching Baidu.
```

```
root@kali: /home/capsersudo
* [theHarvester]                     *
* [theHarvester]                     *
* [theHarvester]                     *
* theHarvester 4.6.0                  *
* Coded by Christian Martorella       *
* Edge-Security Research              *
* cmartorella@edge-security.com       *
*                                     *
*****

[*] Target: britam.com
[*] Searching Baidu.
[*] No IPs found.
[*] No emails found.
[*] No hosts found.

(root@kali) - [/home/capsersudo]
#
```

Ilya otaga

## TASK 4 gather information using deep and dark web search

Hidden Wiki and Exonerator were explored. Since our target organization doesn't have a hidden wikipedia or fakeIDs we decided to move on the next task



The screenshot shows the homepage of TheHiddenWiki.org. The header features the site's name and a search bar. Below the header, there are navigation links for 'HIDDEN WIKI' and 'MORE DEEP WEB ARTICLES', along with an 'RSS FEED' button. The main content area displays a post titled 'Hidden Wiki' dated 2021-06-21. The post includes a category, tags, and a comment section. The text of the post discusses browsing .onion deep web links and installing the Tor browser from the official website. It also lists new .onion links for 2021, including 'OnionLinks v3' and 'Another Hidden Wiki'. A sidebar on the right titled 'Recent Posts' lists several recent updates, including new hidden service domains, a 2021 update, downtime information, a server move, and a Silk Road 2 shutdown notice.

### Hidden Wiki – TheHiddenWiki.org

The darknet guide – The Hidden Wiki

SEARCH

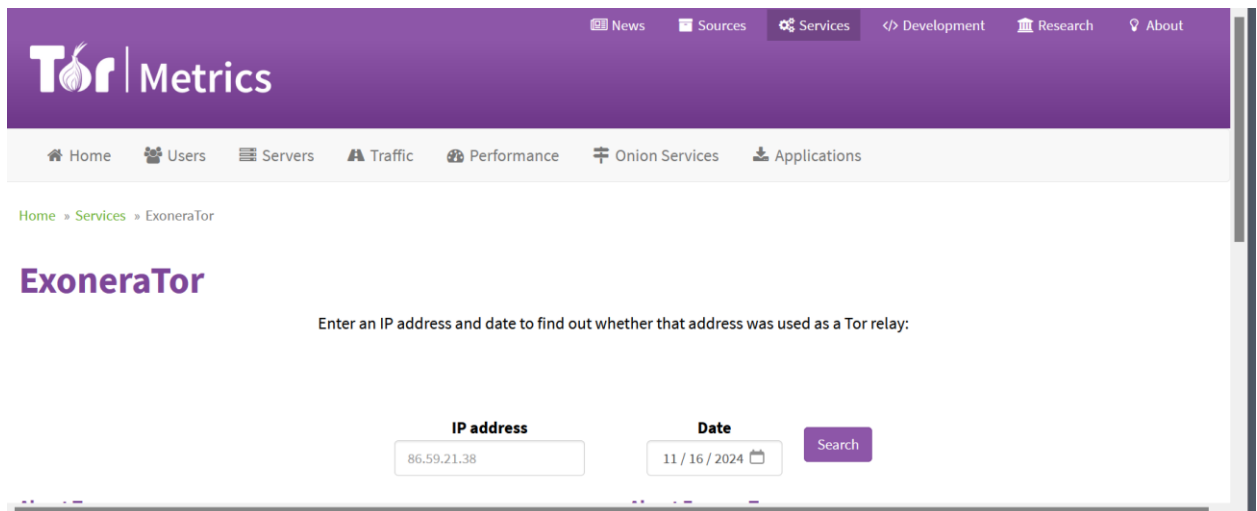
HIDDEN WIKI MORE DEEP WEB ARTICLES RSS FEED

**2021 06.21 Hidden Wiki**  
Category: / Tags: no tag / Add Comment

To browse .onion deep web links, install Tor browser from <http://torproject.org/>  
If you are looking for the best dark web sites, the Hidden Wiki has them all in one place.

**New .onion links 2021**  
**Hidden Wiki sites**  
<http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jppqkvwwqtyd.onion/> – OnionLinks v3  
<http://6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommmfjz3wkhalzgjqxzd.onion/> – The Hidden Wiki  
<http://2jwcnprqbugvyi6ok2h2h7u26qc6j5wxm7feh3znih2qu3h6hld4kyd.onion/> – Another Hidden Wiki

**Recent Posts**  
New type of hidden service domains and other news December 10, 2021  
2021 Hidden Wiki update June 22, 2021  
Recent downtime of the hidden wiki in march 2017 May 8, 2017  
The Hidden Wiki 2015 January 8, 2015  
thehiddenwiki.org moved to a new server because of DDOS January 8, 2015  
Silk Road 2 not shut down and owner



The screenshot shows the Exonerator tool on the TorMetrics website. The header includes the TorMetrics logo and navigation links for News, Sources, Services, Development, Research, and About. Below the header, there is a secondary navigation bar with links for Home, Users, Servers, Traffic, Performance, Onion Services, and Applications. The main content area is titled 'Exonerator' and includes a brief description: 'Enter an IP address and date to find out whether that address was used as a Tor relay:'. Below this, there are input fields for 'IP address' (containing '86.59.21.38') and 'Date' (containing '11 / 16 / 2024'), along with a 'Search' button.

### TorMetrics

News Sources Services Development Research About

Home Users Servers Traffic Performance Onion Services Applications

Home » Services » Exonerator

## Exonerator

Enter an IP address and date to find out whether that address was used as a Tor relay:

**IP address** **Date**

86.59.21.38 11 / 16 / 2024

Search

TASK 5 determine target os through passive footprinting

Censys.io we were able to find Britam Holdings Limited IP addresses Nairobi, Muranga, Machakos and the UK

censys

Hosts

britam.com

Search

Register  
Log In

Results

Report Docs Subscriptions

Host Filters

Labels:

5 jquery

5 network-administration

4 bootstrap

4 remote-access

3 default-landing-page

More

Autonomous System:

10 Britam-Holdings-Limited

6 AMAZON-02

3 SAWASAWA

2 GOOGLE-CLOUD-PLATFORM

1 MICROSOFT-CORP-MSN-AS-BLOCK

Hosts

Results: 24 Time: 0.02s

196.41.68.106

Britam-Holdings-Limited (327994)

Nairobi County, Kenya

443/HTTP

196.41.68.15

Cisco Adaptive Security Appliance

Britam-Holdings-Limited (327994)

Machakos County, Kenya

network.device

network.device.firewall

80/HTTP

443/HTTP

500/IKE

196.41.68.249

Microsoft

Britam-Holdings-Limited (327994)

Nairobi County, Kenya

blazor

jquery

443/HTTP

We chose to explore on Nairobi IP address **196.41.68.106** and found they use default port

censys

Hosts

196.41.68.106

Search

Register  
Log In

Summary History WHOIS Explore

Raw Data

Basic Information

Forward DNS autexpres.britam.com

Routing 196.41.68.0/24 via Britam-Holdings-Limited, KE (AS327994)

Services (1) 443/HTTP

HTTP 443/TCP

11/17/2024 22:30 UTC

Software

VIEW ALL DATA

GO

nginx

Details

https://196.41.68.106/

Status 404 Not Found

Body Hash sha1:5e155cb5551267a9c1371a9c5c8c5b90353c43f9

nsferring data from maxcdn.bootstrapcdn.com...

Geographic Location

City Nairobi

Province Nairobi County

Country Kenya (KE)