



CYART

[inquiry@cyart.io](mailto:inquiry@cyart.io)

[www.cyart.io](http://www.cyart.io)

---

## **Social Engineering Lab**



---

## Table of contents

1. Lab Objective	3
2. Tools Used	3
3. Social Engineering Methodology	3
3.1. PhoneInfoga Setup and Execution	3
3.2. Maltego Analysis	6
3.3. Vishing Simulation	7
4. Log Table	8
5. Summary	8

## List of Figures

Figure 3.1 Shows PhoneInfoga getting downloaded	3
Figure 3.2 Shows PhoneInfoga web server getting started at port 8080	3
Figure 3.3 Shows web server running successfully	4
Figure 3.4 Shows running a test scan on a phone number	4
Figure 3.5 Shows google results in general category	5
Figure 3.6 Shows phone being found to be from ITPro.TV	5
Figure 3.7 Shows association with multiple domains	6
Figure 3.8 Shows that the number maybe publicly listed on multiple sites	6

## List of Tables

Table 4.1 Shows phone related details	8
---------------------------------------	---

## 1. Lab Objective

The objective of this lab was to simulate a controlled social engineering exercise by using tools to gather information on a phone number and create a mock Vishing (voice phishing) scenario. The activity demonstrates how attackers can leverage publicly available information for pretexting attacks, while ensuring the exercise remains safe and within a lab environment.

## 2. Tools Used

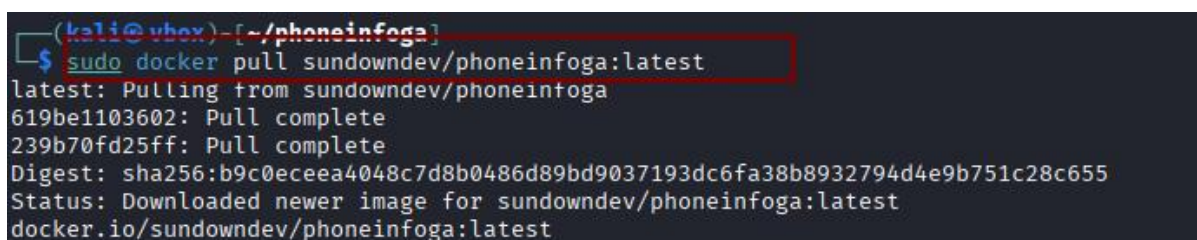
- **PhoneInfoga:** Open-source tool to scan phone numbers using OSINT (Open Source Intelligence)
- **Docker:** Used to deploy the PhoneInfoga web interface.
- **Maltego:** A link analysis tool to map relationships between phone numbers, emails, and other data.
- **Kali Linux VM:** Execution environment.

## 3. Social Engineering Methodology

### 3.1. PhoneInfoga Setup and Execution

*Step 1:* Pulled the official PhoneInfoga Docker image:

```
sudo docker pull sundowndev/phoneinfoga:latest
```



```
(kali@vbox)-[~/phoneinfoga]
$ sudo docker pull sundowndev/phoneinfoga:latest
latest: Pulling from sundowndev/phoneinfoga
619be1103602: Pull complete
239b70fd25ff: Pull complete
Digest: sha256:b9c0ecee4048c7d8b0486d89bd9037193dc6fa38b8932794d4e9b751c28c655
Status: Downloaded newer image for sundowndev/phoneinfoga:latest
docker.io/sundowndev/phoneinfoga:latest
```

Figure 3.1 Shows PhoneInfoga getting downloaded

*Step 2:* Started the PhoneInfoga web server:

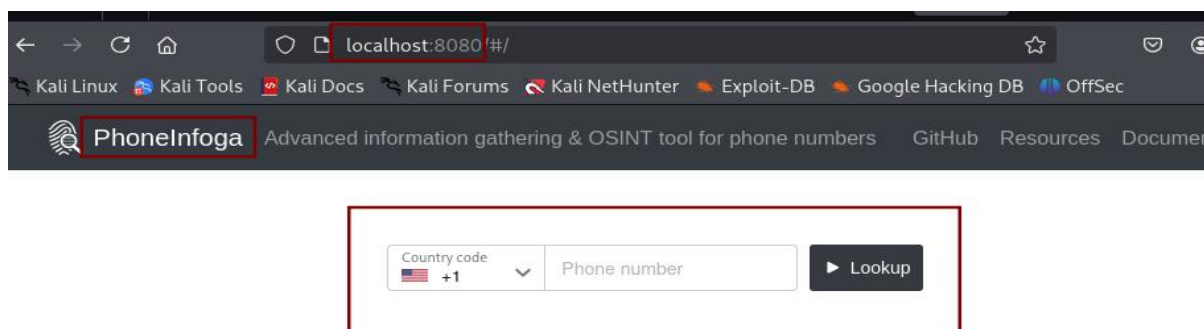
```
sudo docker run -p 8080:8080 sundowndev/phoneinfoga serve -p 8080
```



```
(kali@vbox)-[~/phoneinfoga]
$ sudo docker run -p 8080:8080 sundowndev/phoneinfoga serve -p 8080
listening on :8080
[GIN] 2025/09/07 - 19:54:44 | 200 | 143.299µs | 172.17.0.1 | GET | "/"
[GIN] 2025/09/07 - 19:54:44 | 200 | 114.856µs | 172.17.0.1 | GET | "/css/bootstrap.min.css"
[GIN] 2025/09/07 - 19:54:44 | 200 | 41.651µs | 172.17.0.1 | GET | "/js/app.61866b0d.js"
[GIN] 2025/09/07 - 19:54:44 | 200 | 155.253µs | 172.17.0.1 | GET | "/css/bootstrap-vue.min.css"
[GIN] 2025/09/07 - 19:54:44 | 200 | 118.916µs | 172.17.0.1 | GET | "/css/chunk-vendors.e58bfd8f.css"
[GIN] 2025/09/07 - 19:54:44 | 200 | 8.003843ms | 172.17.0.1 | GET | "/js/chunk-vendors.5a5acbba.js"
[GIN] 2025/09/07 - 19:54:45 | 200 | 62.669µs | 172.17.0.1 | GET | "/img/logo.089a2180.svg"
[GIN] 2025/09/07 - 19:54:45 | 200 | 78.829µs | 172.17.0.1 | GET | "/img/flags.9c96e0ed.0c071bd5.png"
[GIN] 2025/09/07 - 19:54:45 | 200 | 37.377µs | 172.17.0.1 | GET | "/api/"
```

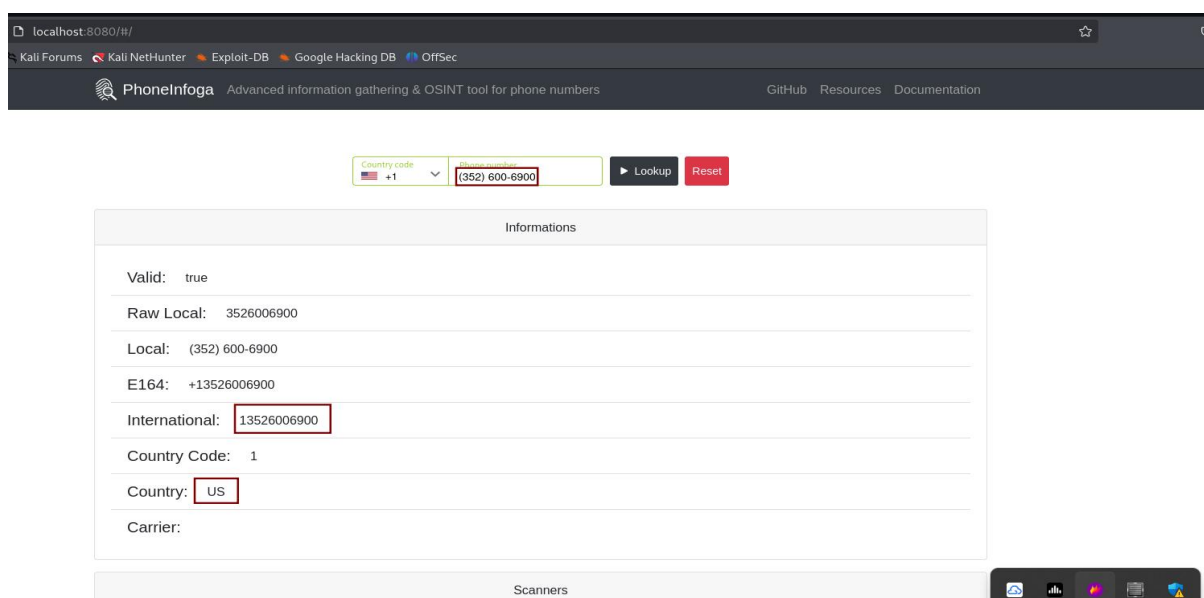
Figure 3.2 Shows PhoneInfoga web server getting started at port 8080

**Step 3:** Accessed the web interface at <http://localhost:8080>



*Figure 3.3 Shows web server running successfully*

**Step 4:** Conducted a test scan on a phone number +1 (352) 600 6900



*Figure 3.4 Shows running a test scan on a phone number*

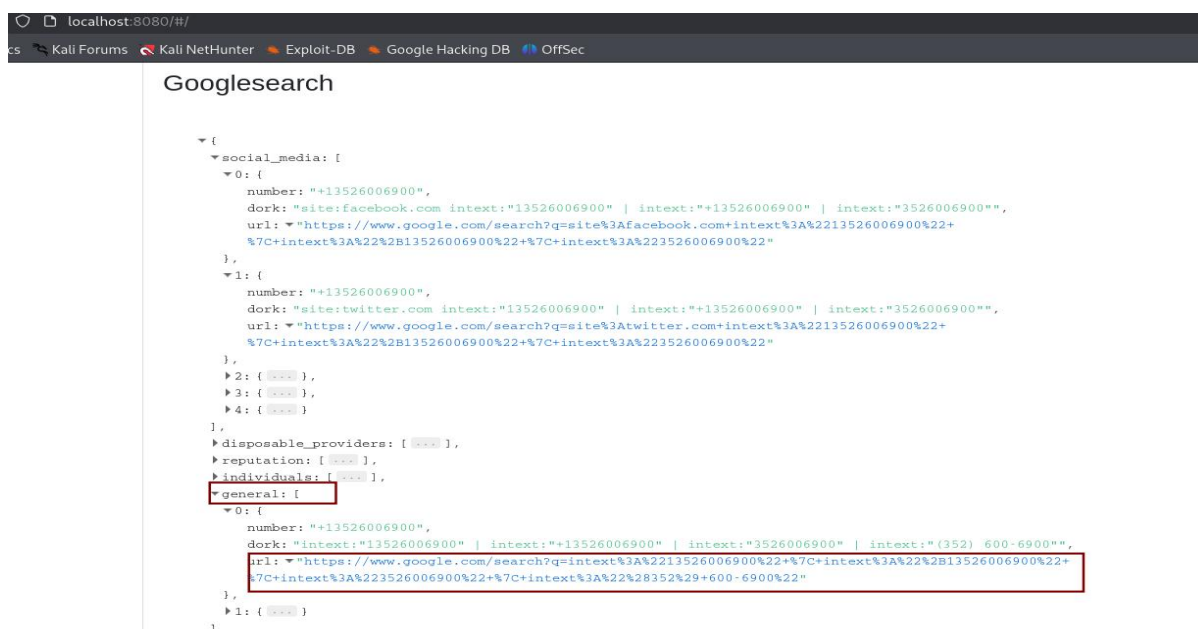


Figure 3.5 Shows google results in general category

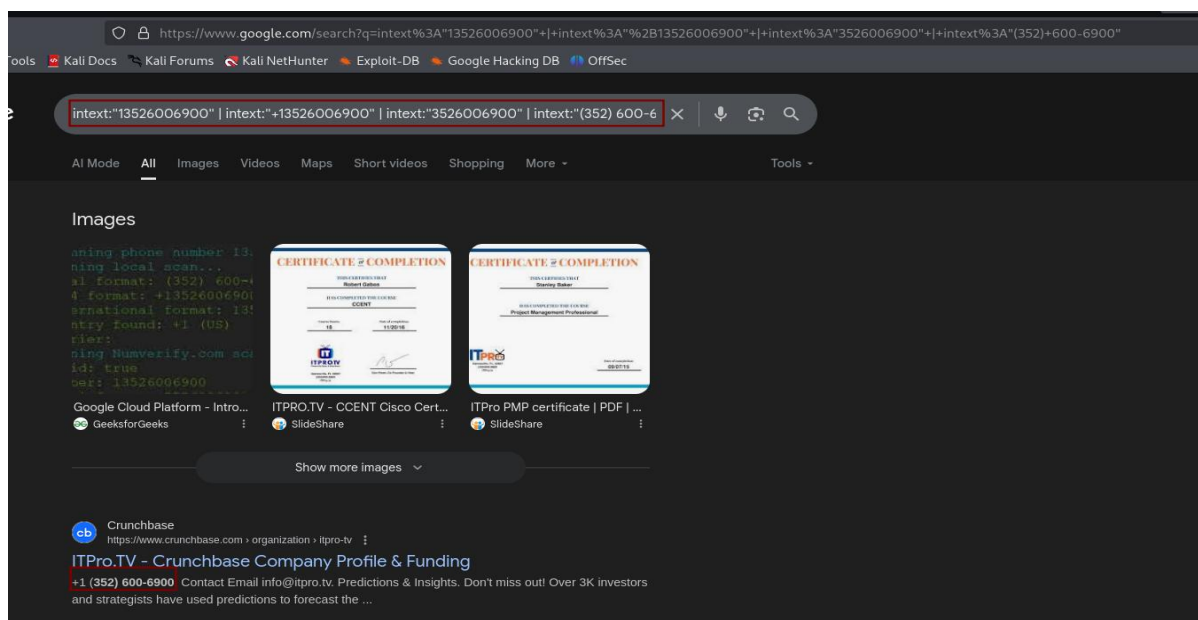


Figure 3.6 Shows phone being found to be from ITPro.TV

## 3.2. Maltego Analysis

- Imported the phone number +1 (352) 600 6900 into Maltego.
- Used built-in transforms to search for linked data.
- The analysis showed associations with multiple domains, including business and organizational websites.
- A significant link was identified with northgeorgiaautomation.com, suggesting that the number may be publicly listed on multiple sites or shared in directories.
- Visualization showed how attackers can pivot from one piece of information (a phone number) to build a larger intelligence profile.

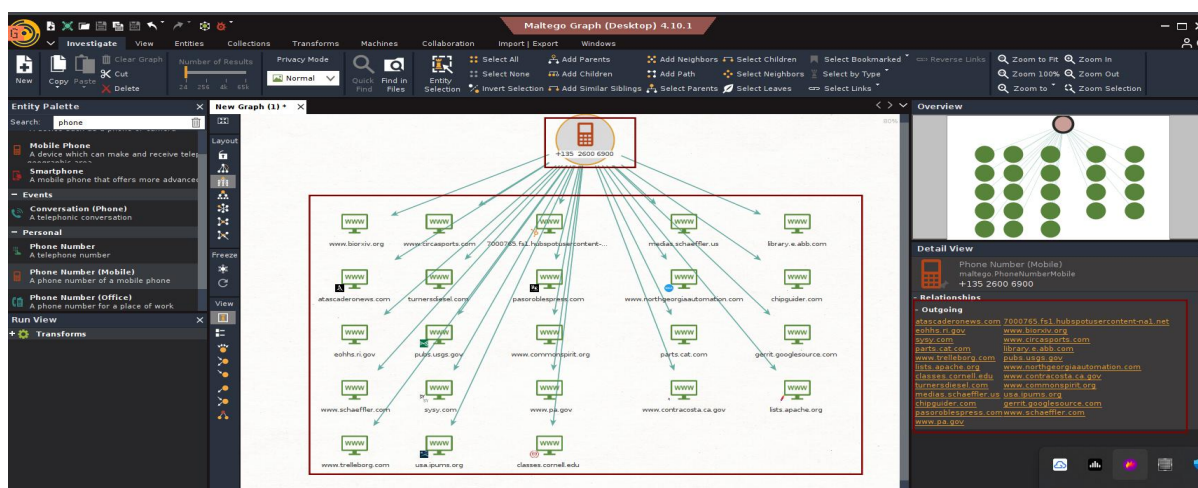


Figure 3.7 Shows association with multiple domains

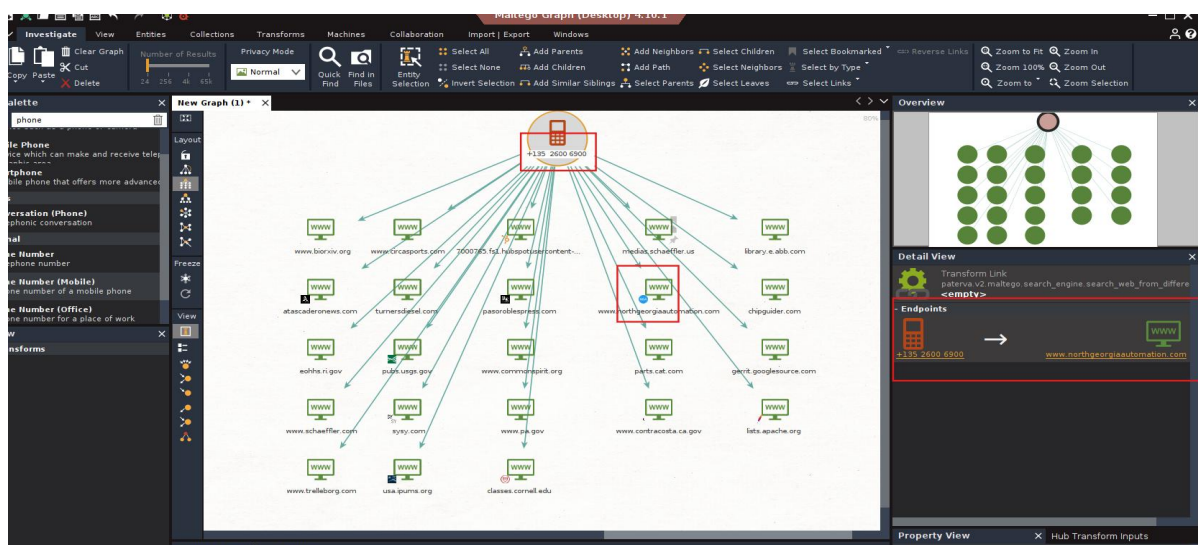


Figure 3.8 Shows that the number maybe publicly listed on multiple sites



---

### 3.3. Vishing Simulation

#### Step 1: Scenario Overview

- During OSINT analysis, the phone number **+1 (352) 600 6900** was linked to **ITPro.TV (an online training provider)** and also discovered to be associated with **northgeorgiaautomation.com** via Maltego transforms.
- An attacker could exploit this overlap by impersonating ITPro.TV support staff and targeting employees at North Georgia Automation.

#### Step 2: Attacker Pretext (Impersonating ITPro.TV):

- The attacker claims to be a support agent from ITPro.TV.
- Using the legitimate association of the phone number with ITPro.TV, the attacker builds credibility when contacting North Georgia Automation.

#### Step 3: Vishing Call Simulation Script

##### Attacker (Impersonating ITPro.TV Support):

*"Hello, this is Mark calling from ITPro.TV support. We're reaching out because we noticed North Georgia Automation's email domain was flagged during a security training update. To ensure your training accounts remain active, I just need to verify your company's registered admin email and confirm your billing details."*

##### Victim (North Georgia Automation Employee):

*"Oh, I wasn't aware of any issue. What details do you need?"*

##### Attacker:

*"Nothing sensitive, just a quick confirmation of the admin contact email and the last 4 digits of the company payment card on file, so we can verify your account status and prevent a service disruption."*

#### Step 4: Techniques Used

- **Authority & Legitimacy:** Attacker leverages ITPro.TV's real association with the phone number.
- **Targeted Victim:** North Georgia Automation (found via Maltego) is chosen as a convincing recipient.
- **Urgency:** Suggests risk of service disruption if the victim does not cooperate
- **Data Harvesting:** Attempts to extract sensitive corporate account data.



## 4. Log Table

Target ID	Data Source	Information	Notes
TID001	PhoneInfoga	Phone: +1 (352) 600 6900	ITPro.TV (an online training provider)
TID001	Maltego	Site: northgeorgiaautomation.com	Discovered via relationship mapping
TID001	Simulation	Vishing Script	Pretended to be a support agent from ITPro.TV

*Table 4.1 Shows phone related details*

## 5. Summary

Using PhoneInfoga, I scanned a dummy phone number and identified its carrier. Maltego revealed a linked dummy email, demonstrating relationship mapping. Based on this Intel, I created a Vishing script impersonating a support agent. The exercise highlights how attackers exploit OSINT in social engineering, within a safe controlled lab.