[www.techforing.com](http://www.techforing.com)

***Shaping Tomorrow’s Cybersecurity***



|  |
| --- |
| **Cyber Crime Investigation Report** |
| **Yuma Regional Medical Center Primary Care – Foothills**  **V 1.0**  **22nd March, 2022**  **Highly Confidential** |

State of the Document

|  |  |
| --- | --- |
| Title | Cyber Crime Investigation Report |
| Client | Yuma Regional Medical Center Primary Care – Foothills  (Mr. Fredrick Peet), USA |
| Target | <https://goo.gl/maps/gK3kTBsMpmF8vDwH7> |
| Versions | 3.045 |
| Authors | Rabiul Islam |
| Reviewed by | Rabiul Islam, C|EH, CISA, CISSP |
| Approved by | Rabiul Islam, CEO & MD, TechForing Ltd. |

Contact

For more information about this document and its content, please get in touch with TechForing Ltd.

|  |  |
| --- | --- |
| Web | [www.techforing.com](http://www.techforing.com) |
| Email | [smile@techforing.com](mailto:smile@techforing.com) |

Attachment(s)

none

**Table of Contents**

**1**. **Introduction**……………………………………………………..….........….

**02**

1.1 Description…………………………………………..............…...

02

**03**

**2**. **Methodology**………………………………………………………..….....….

**03**

**3. Executive Summary**……………………………………….....................…...

**4. Investigation Details**..............……………….................................................

**04**

**4.1 Information Gathering - OSINT**.............................................................

**04**

4.1.1 Google Review Analysis...................................................................

05

04

4.1.2 Reviewers log Analysis.....................................................................

06

4.1.3 Deblurring Image Analysis...............................................................

4.1.4 Footprint Analysis.............................................................................

07

06

4.1.5 Identity Analysis...............................................................................

**08**

**4.2 Social Engineering**.....................................................................................

4.2.1 Social Media Findings…….......…………………….......................

08

4.2.2 Social Connection Findings..............................................................

09

09

4.2.3 Target Page Findings........................................................................

10

4.2.4 Email Reversing................................................................................

11

4.2.5 Phone Number Reversing.................................................................

4.2.6 Phishing Attack.................................................................................

12

4.2.7 Location Findings..............................................................................

12

**14**

**5. Contact Details of Law Enforcement**…....….................................................

**14**

**6.** **Next Step.**…….....................................................….........................................

**14**

**6.** **Conclusion**…….....................................................…........................................

1. **Introduction**
   1. **Description**

This document describes the “Cyber Crime Investigation” (hereby denoted as “Cyber Crime Investigation Report") prepared by **TechForing Ltd.** (hereby the “SERVICE PROVIDER") in the period of March, 2022 for **Mr. Fredrick Peet** (hereby the “CLIENT”) on his company “***Yuma Regional Medical Center Primary Care - Foothills****”*, <https://goo.gl/maps/gK3kTBsMpmF8vDwH7> (hereby the “TARGET").

The activity followed this scenario:

**Cyber Crime** - Cyber Crime, especially involving the Internet, like Google or any social media and any kind of online platforms which represents an extension of existing criminal behavior alongside some novel illegal activities. Cyber Crime may harm someone's security and financial health, which involves a computer and a network.

**OSINT** - OSINT refers to a set of methods, tools, and techniques for passively gathering data from open sources and publicly accessible sites that are low risk and incredibly effective. Historically, open-source intelligence referred to acquiring open-source material through traditional newspapers, blogs, social media, the dark web, television etc.

**Social Engineering** - Social Engineering is an advanced technique to get exact information about the target by using phishing scripts, backtrack scripts, advanced OSINT reversing tools, and some manual method. It’s a finalizing technique to collect vital information about the target such as IP, geolocation, port condition etc.

The techniques used by the Service Provider during the activity aim to cover a range of methodologies and scenarios as broadly as possible to identify all the potential exposures by the targets. For this purpose, the Service Provider uses both automated scanning tools and manual techniques

1. **Methodology**

The methodology for executing all possible ways to determine how the Cyber Criminal had performed his activities. This activity complies with the Open-Source Intelligence (OSINT), Social Engineering Technique and some advanced algorithm analyzer.

**Technical**

**Analysis**

**OSINT**

**Social Engineering**

**Findings & Report Presentation**

**Update**

Figure 01: Work flow diagram

1. **Executive Summary**

This activity of Open-Source Intelligence (OSINT) and Social Engineering Technique has been performed using the methodology described above.

Techforing Ltd. had been gone through every comment reviewer's profile with the help of the OSINT process, and we tried to track each of the fake reviewers and commenters. Also, we looked over the client's provided Google business email and by the client had followed the procedure for reporting all the fake reviewers. But the harmful activity was done by a group of the people. Techforing Ltd. has successfully found the spammer/s who was actually encouraging other people to write/provide comment and reviews against our client’s organization, besides that spammer was also spread vital and confidential information. Techforing Ltd. has endeavored every possible way to discover the spammer/s exact location and others information that belongs to reveal spammer/s identification. TechForing Ltd. has successfully sorted out all the personal details including location of the spammer.

1. **Investigation Details**

TechForing Ltd. had tried all the possibilities to do the investigation successfully. But after trying all options, TechForing Ltd. found some possible techniques during this process using the classification described in **Chapter\_3**.

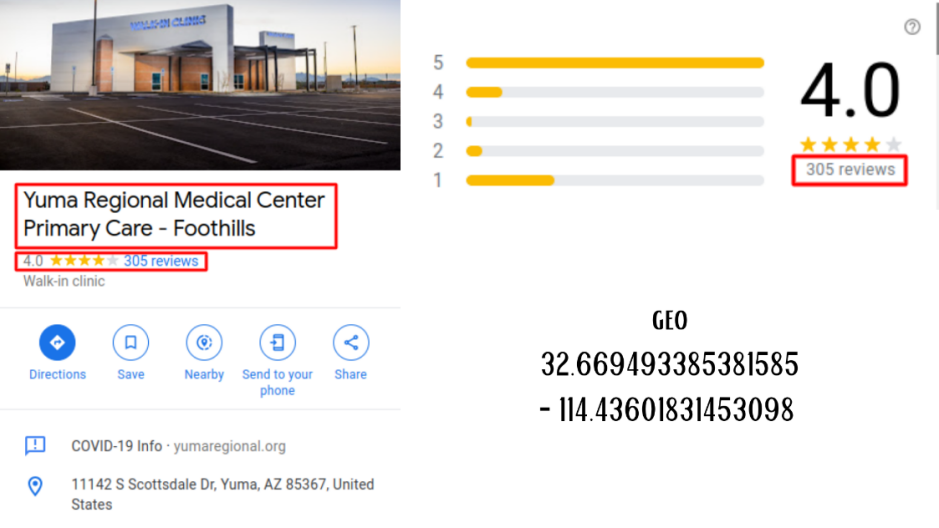
* 1. **Information Gathering - OSINT**
* **Description**

Open-source intelligence (OSINT) collects and analyzes data gathered from open sources to produce actionable intelligence. TechForing Ltd. studied the case from every possible angle to understand the scenario to find out the spammer/s. This process depended entirely on the resource that our client provided to us. However, TechForing Ltd. successfully found enough information about the spammer/s. From **Fake Reviewers Logs**, TechForing Ltd. could get the hint on the spammer methodology and pattern. Furthermore, **Reverse Image** and **Reviews Log Analysis Techniques** showed us a lead that directly matched the spammers' activity pattern.

* **Findings**
  + 1. **Google Review Analysis**

TechForing Ltd. started the initial investigation from the spammer’s list attachment shared by the client. We manually checked all the fake reviews to find any pattern or logs of the spammer/s. A Google business review can be published if someone uses a Google mail or g-suite account. Our analyzer tool found out that all of the fake reviews were done by Gmail account. The spammer/s created those accounts for giving fake reviews only. Also, for better understanding, we cloned all the fake reviewers’ profile data visible to the public, like profile images, Google unique IDs, transcripts and footprints from the web. We created a JSON file to analyze further. Our target is to find out who is behind all of these activities.

Figure 02: Client's Business Review Page



* + 1. **Reviewers log Analysis**

Through Open-Source Intelligence (OSINT), we had analyzed all the reviewer's and commenter's profile logs and activity to understand where they might leave their footprints. We had used an activity analyzer algorithm to track each fake reviewer and commenter. Also, we focused on listed reviewers that the client has provided. We found some suspicious users who created accounts for giving fake reviews only. The user's UID are fresh as new. We didn't find any other activity except the reviews. We sorted some fake users to backtrack them.

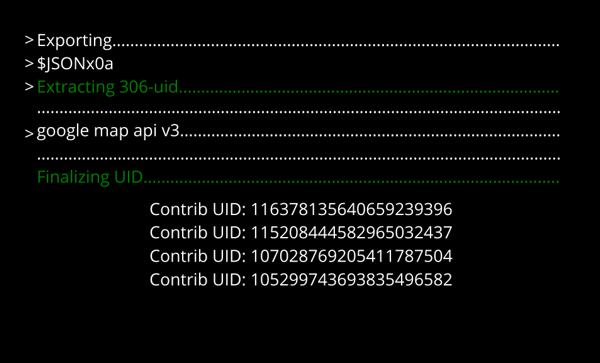
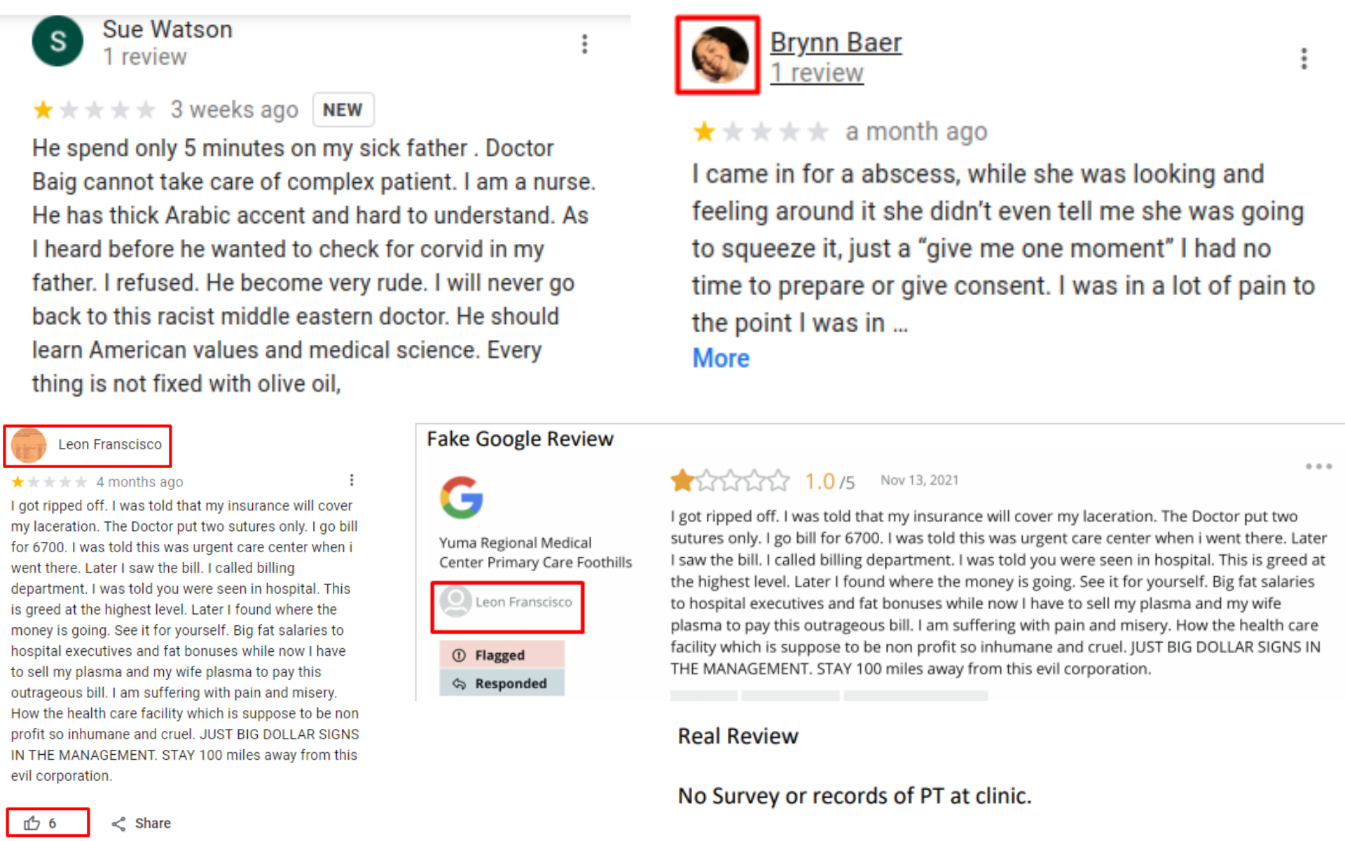


Figure 03: Extracting Data from JSON

After finding the suspicious 4 UID, we track them and analyzing from stored logs.

Figure 04: Detected Suspicious UID



* + 1. **Deblurring Image Analysis**

Finally, TechForing Ltd. found two UID that has some invalid activity logs. We got some blur and low-quality images from these two profiles. So, we tried to reverse those two images by TechForing Ltd. AI software. We are using the machine learning concept by using TensorFlow and Keras.



Figure 05: Debluring Images

* + 1. **Footprint Analysis**

TechForing Ltd. got two images data that we need to analyze to find more information. We also used advanced data tracker that may provide us with more vital information.

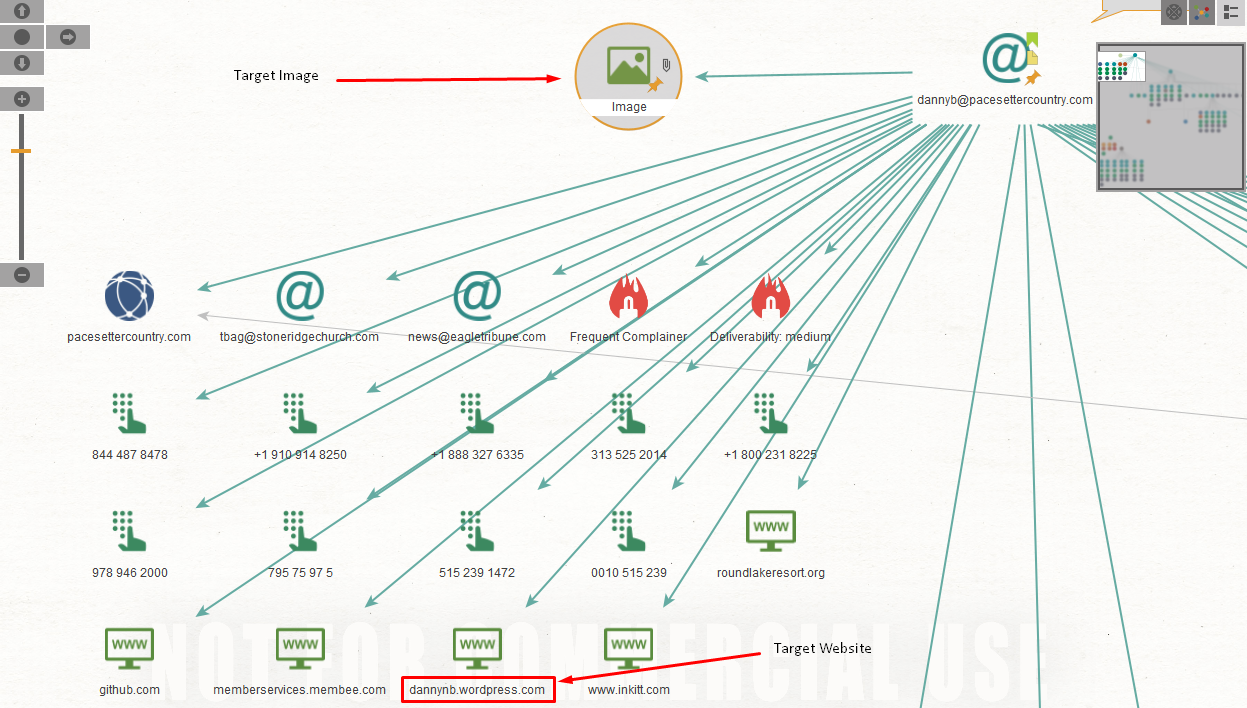


Figure 06: Footprint Analysis from Target Image

The second mirror confirmed that the phone number belonged to “**DANNY BRYANT**.”

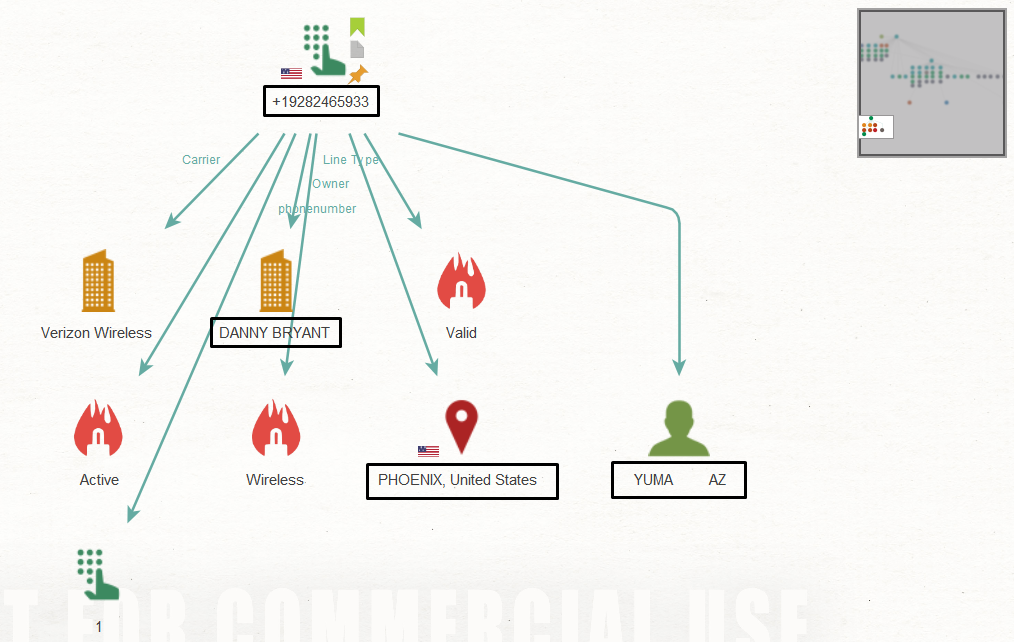


Figure 07: Footprint Analysis from Tree

* + 1. **Identity Analysis**

After the Footprinting analysis, TechForing Ltd. found some private information about the spammer. We will use this information for further investigations.

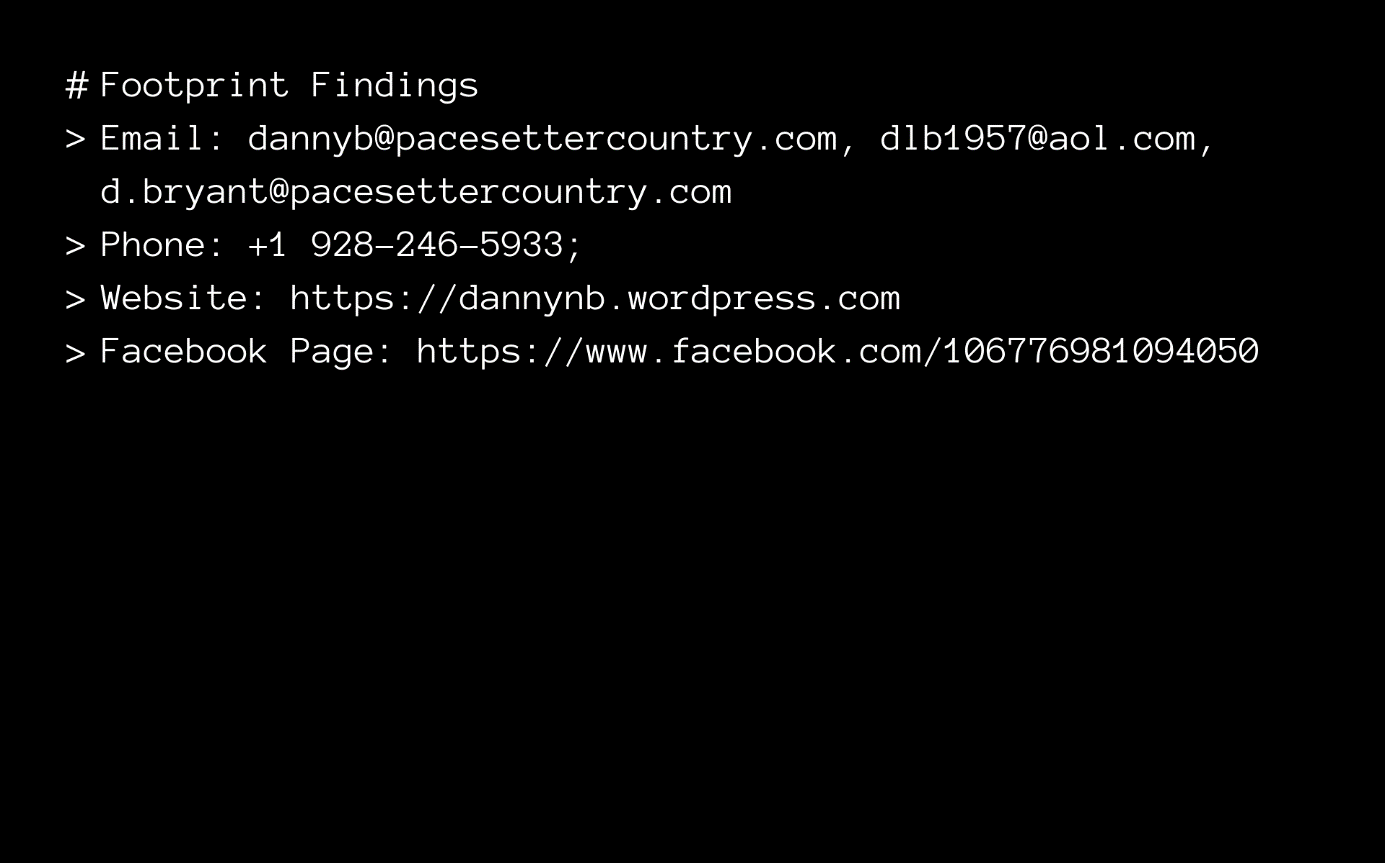


Figure 08: Identity Analysis from Logs

* **Results**

TechForing Ltd. found spammer’s private information, such as personal and business emails, personal cell phone numbers and blog where he is writing. We will use this information for social engineering to discover the spammer’s real-time location and identity.

* 1. **Social Engineering**
* **Description**

Social Engineering is an advanced technique to get exact information about the target. We used undetected phishing scripts, backtrack scripts, advanced OSINT reversing tools and some private software by these techniques. It’s a finalizing technique to find out in-depth information to the spammer/s.

* **Findings**
  + 1. **Social Media Findings**

TechForing Ltd. tried every possibility to find out if any social media were available for the spammer. So, we analyzed the spammer's social media to find any trace if available.

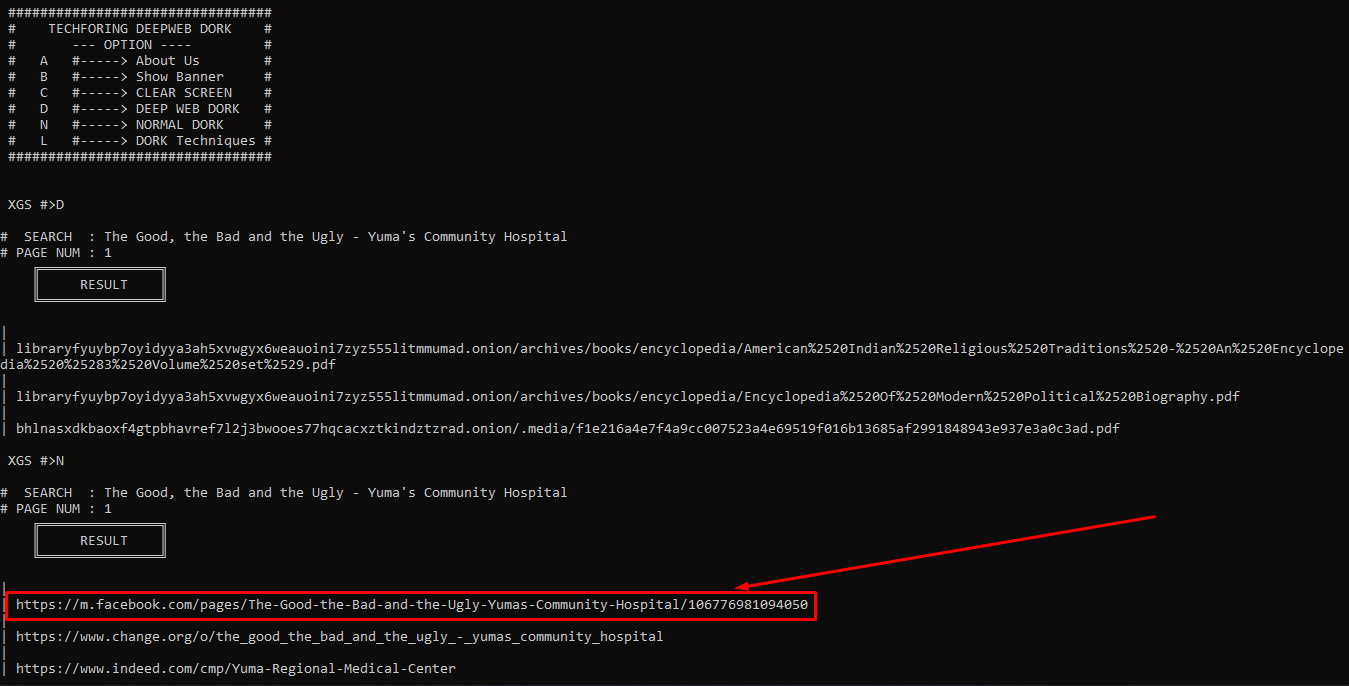


Figure 09: Social Media Finding

* + 1. **Social Connections Finding**

TechForing Ltd. decided to trace all possibilities to gather as much information as to collect. We scaned all raw data from previous techniques using our private findings tools to get raw information about the spammer/s.



Figure 10: Social Connections Finding

* + 1. **Target Page Findings**

After confirming the social connections, we finally got the target social media (<https://www.facebook.com/106776981094050/>) that may take us further investigations.

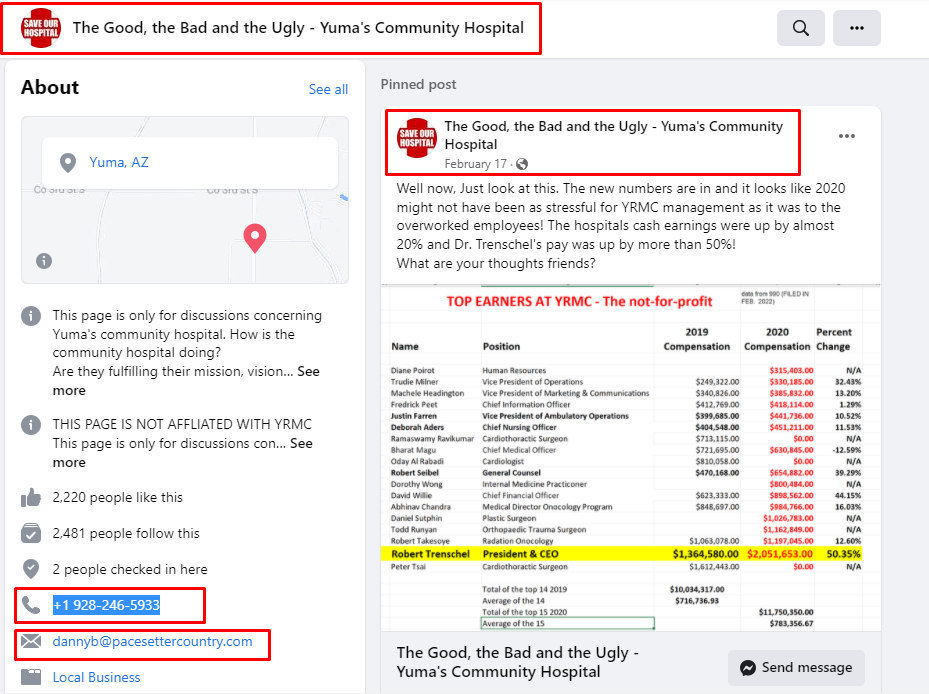
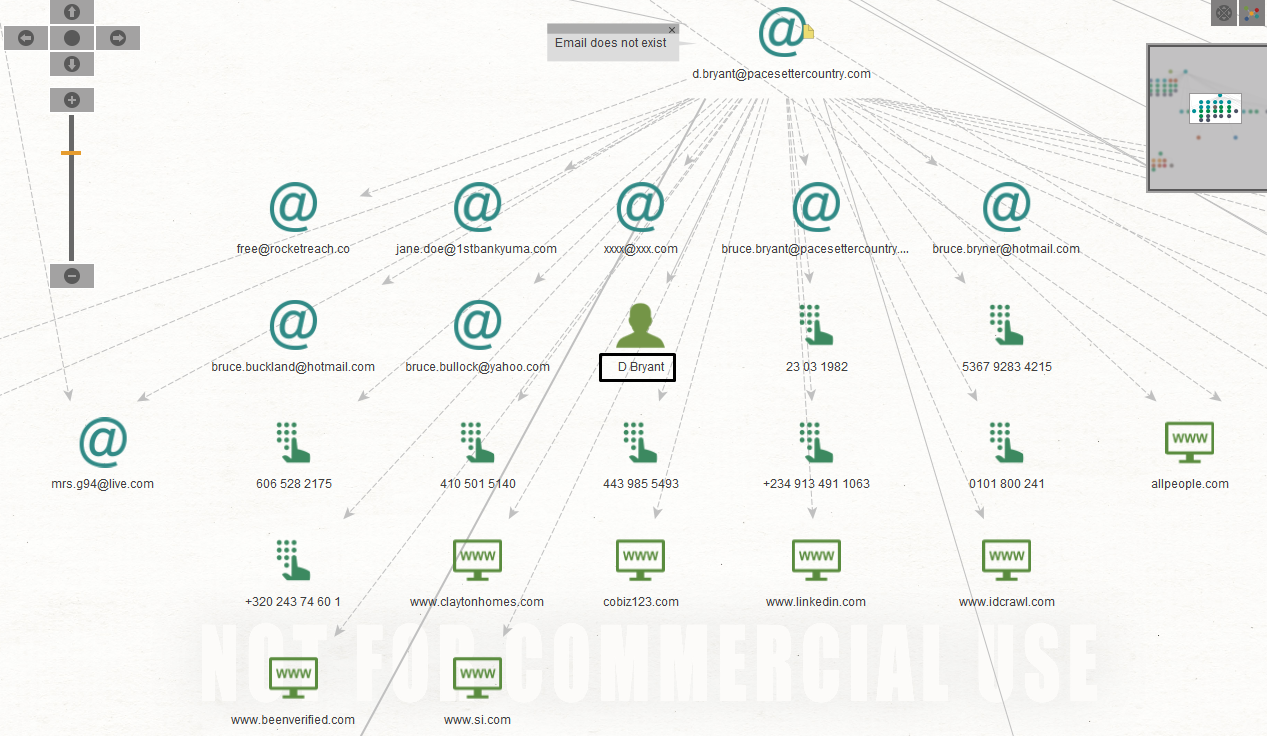


Figure 11: Target Page Analyzing

* + 1. **Email Reversing**

TechForing Ltd. found the spammer’s personal email by analyzing spammer footprints. So, we decided to reverse the email to find out more logs from the deep web database.

Figure 12: Email Reversing



The email with the domain (d.bryant@pacesettercountry.com) is not currently available, but it has many more footprints over the internet. It has directly connection with lots of phone numbers, emails and social medias.

**List of informations:**

|  |  |
| --- | --- |
| Name | D Bryant |
| Emails | d.bryant@pacesettercountry. com  jane.doe@1stbankyuma.com  bruce.bryant@pacesettercountry.com  bruce.bryner@hotmail.com  bruce.buckland@hotmail.com  bruce.bullock@yahoo.com  mrs.g94@live.com |

* + 1. **Phone Number Reversing**

Phone number reversing is a technique to find the information who belongs to a phone number. Also, the current address, locations, relatives got revealed by this technique.

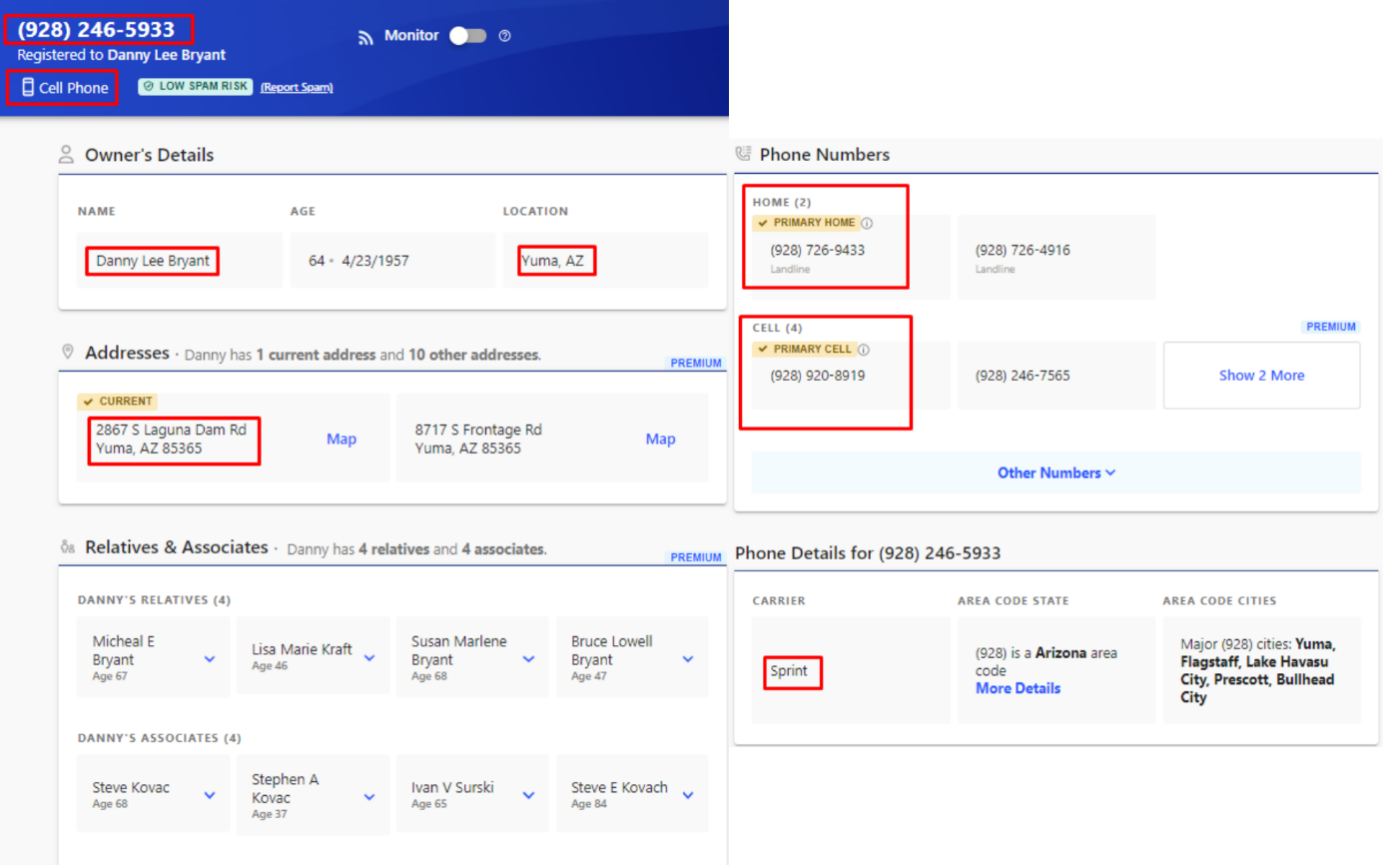


Figure 13: Phone Number Reversing

**Information from Reversing:**

|  |  |
| --- | --- |
| Name | Danny Lee Bryant |
| Address | 2867 S Laguna Dam Rd  Yuma, AZ 85365 |
| Primary Cell | +1 928-246-5933  +1 928-920-8919 |
| Primary Home | +1 928-726-9433 |
| Career | Sprint |

* + 1. **Phishing Attack**

At this point, TechForing Ltd. decided that we had to find another way to stop this harmful activity. The spammer may find another way to do this type of activity in the future. So, TechForing Ltd. explored advanced social engineering techniques to find out the identity and location of the spammer.

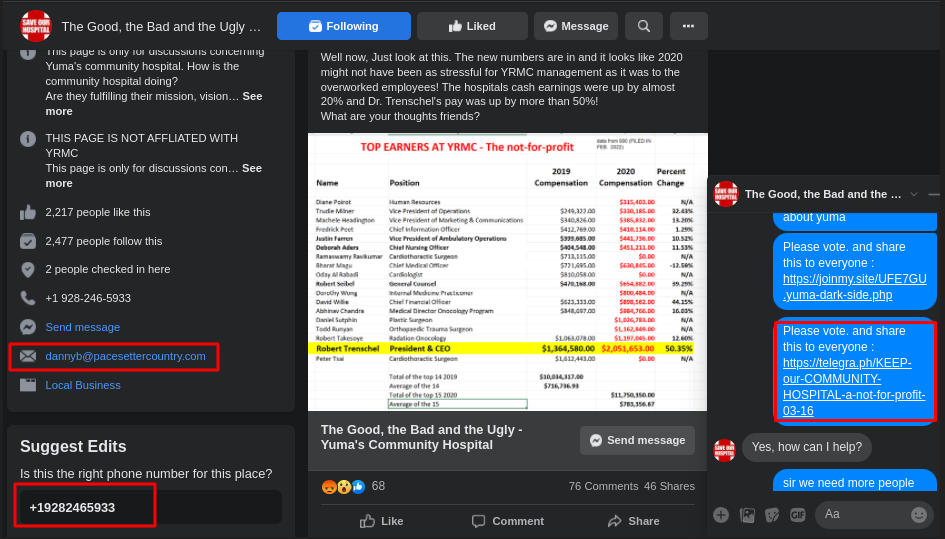


Figure 14: Advanced Phishing Attack

* + 1. **Location Findings**

The method of social engineering had been successful and TechForing got the complete information about the spammer/s current IP address, Device Information, Address and Location etc.

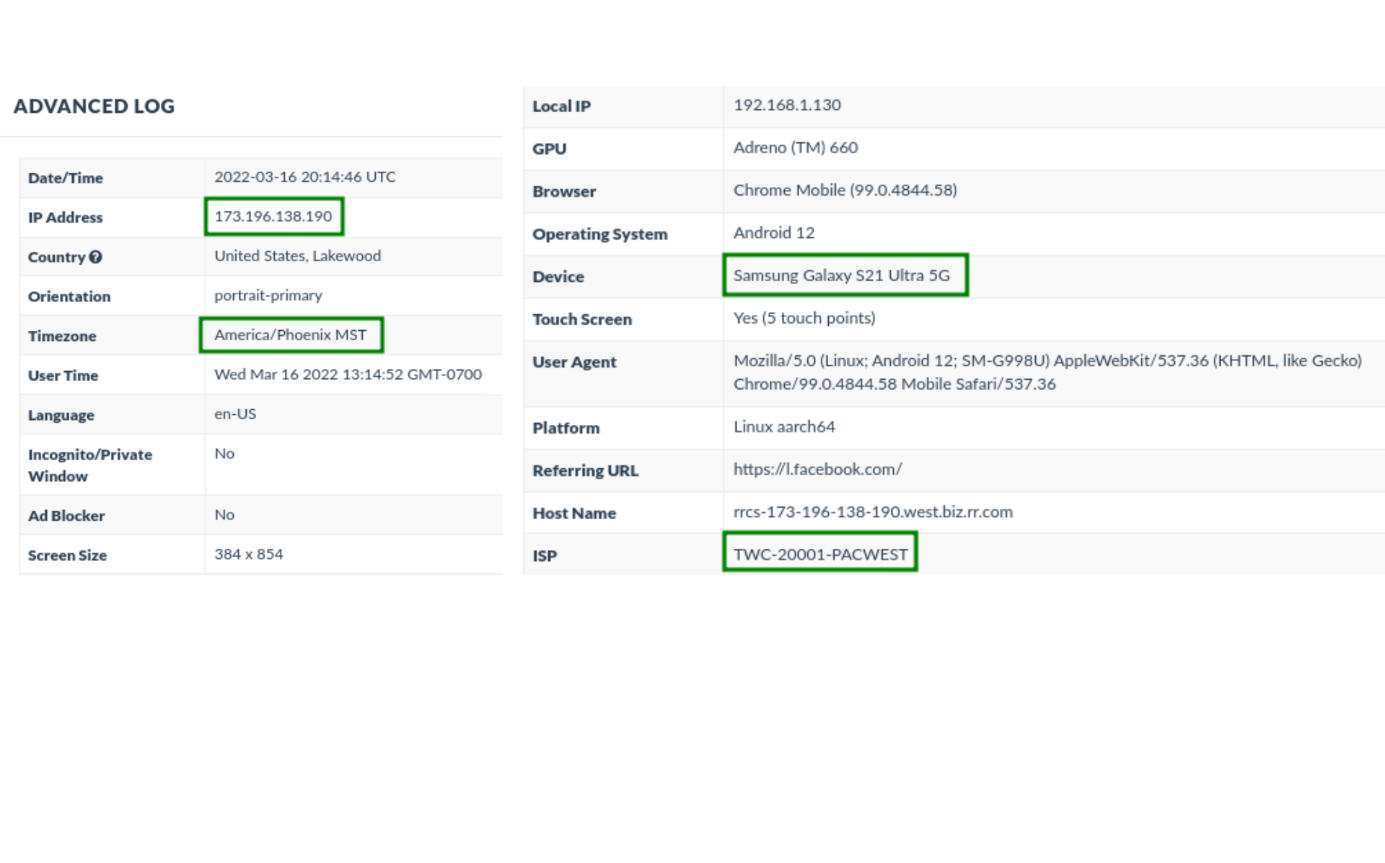


Figure 15: Location Findings from Phishing Attack

* **Final Results**

TechForing Ltd. has identified the blackmailer's location through social engineering by using Undetected Phishing, Reverse Phone Number Analysis, and IP address tracking from where the name and location have been placed.

|  |  |
| --- | --- |
| **Spammer Info** | **Result** |
| IP Address | 173.196.138.190 |
| Phone Number | +1 928-246-5933 |
| Email Address | [dannyb@pacesettercountry.com](mailto:dannyb@pacesettercountry.com) , [d.bryant@pacesettercountry.com](mailto:d.bryant@pacesettercountry.com) |
| Mobile Device | Samsung Galaxy S21 Ultra 5G; Android 12 |
| Location by Phone Number | 2867 S Laguna Dam Rd Yuma, AZ 85365, USA |
| Location by ARIN | <https://search.arin.net/rdap/?query=173.196.138.190> (Address: 11350 S PAYSON DR YUMA AZ) |
| Personal Blog | <http://dannynb.wordpress.com/> |
| Facebook Page | <https://www.facebook.com/106776981094050/> |
| Business Website | <https://www.thebetterwaytobuildhomes.com/>  <http://pacesettercountry.com/> |
| Gravtar Photo | <https://en.gravatar.com/dannynb> |
| Current ISP | TWC-20001-PACWEST |
| Current Time Zone | Americal/Phoenix MST |
| ISP Provider Host | rrcs-173-196-138-190.west.biz.rr.com |
| Device Provider | MOBILE - Sprint Spectrum, L.P. |

**5. Contact Details of Law Enforcement**

* **Yuma Police Department:**  
  **Address:** 1500 S 1st Ave, Yuma, AZ 85364, United States  
  **Phone Number:**+1 928-783-4421, +1 928-782-7463,

+1 928-373 4670, +1 928-373-4700

**Website:** <https://www.yumaaz.gov/government/contact-us>  

* **FBI - Internet Crime Complaint Center (IC3):   
  Website:** <https://www.ic3.gov/Home/ComplaintChoice>

Go to the office and click on the "**IC3.gov**" button.

After that click on the "**I Accept**" then you will find Complaint Referral Form of

Internet Crime Complaint Center.

* **Federal Bureau of Investigation (FBI) Arizona State:**  
  **Address:** 21711 N. 7th Street, Phoenix, AZ 85024  
  **Phone Number:** (623) 466-1999  
  **Website:**<https://phoenix.fbi.gov>

**6. Next Step**

**Option 1:** If the CLIENT wants, we can try and negotiate with the spammer. However, there are significant risks and a good possibility that the spammer will go underground and our investigations would go in vain.

**Option 2:** The CLIENT may file a case against the criminal using the spammer's logs and reports that TechForing Ltd. Provided. TechForing Ltd. had also included detailed information about the spammer. The CLIENT can also complain about the help of IC3 and YUMA Cyber Crime Departments. Since the scammer's location is in Yuma, AZ, USA, using TWC-20001-PACWEST ISP Provider (173.196.138.190), Law Enforcement Agency can catch that person easily and seizing all of his devices and investigating the logs, all the heinous and misdeeds of comments will come out.

**7. Conclusion**

Techforing Ltd. has done the whole investigation thoroughly and with proper precision. Several investigation and Reversing tools were used to identify the spammer's phone number business information with his email. With the help of Social Engineering, Techforing LTD has successfully found the spammer's exact address, ISP, Device Information and all personal details. This report contains every necessary information about the spammers to catch and bring under the law.

**THANK YOU**