IMPLEMENTATION OF ATTACKS ON SIGNALLING SYSTEM NO. 7

The security framework of the Signaling System No. 7 (SS7) protocol is notably deficient, allowing it to be easily compromised by hackers. Due to the absence of robust security mechanisms within the SS7 protocol, individuals with unauthorized access can intercept text messages, eavesdrop on conversations, and pinpoint a user's location. This vulnerability extends to bypassing two-factor authentication by capturing the SMS codes sent to users to verify their identity.

Furthermore, upon intercepting the SMS message, the hacker can gain access to the user's social media platforms, and online banking accounts (Steiner et al., 2019)

Sigploit

SigPloit is a cybersecurity tool designed to test the security of telecommunication systems. It focuses on finding vulnerabilities in protocols like SS7, GTP, and Diameter, which are essential for mobile networks. SigPloit can simulate attacks to show how hackers could track locations, intercept calls, commit fraud, or cause service disruptions. Its purpose is to help improve the security of telecom networks by identifying and addressing these vulnerabilities (Steiner et al., 2019).

Methodology Overview

Simulation Mode

The practice mode is available to help you grasp the intricacies of attacks when direct access to the SS7 network is not possible. Server-side components, found in the directory "SigPloit/Testing/Server/Attacks/", come in the form of .jar files. To simulate an attack on a client system, one should employ the pre-defined values within each server-side component (Mahar, 2021).

Locating a Subscriber

There are a couple of SS7 techniques that allow the determination of a subscriber's geographical position in the global mobile network. Initially, the Any Time Interrogation message is used to gather the subscriber's location details. However, it's worth noting that many network operators have now switched off the response feature to these queries. Following this, the attacker can send Mobile Application Part (MAP) messages by imitating a counterfeit Home Location Register. This method furnishes the attacker with the subscriber's current location based on collected data, including the Cell ID, Mobile Network Code (MNC), Mobile Country Code (MCC), and Location Area Code (Cleary, 2020).

Sigploit Setup

Prerequisites:

1. Python version 2.7
2. Java version 1.7 or higher
3. A Linux-based system

GitHub repository to simulate the attack:
https://github.com/ethicalhackeragnidhra/SigPloit-ss7

Two IPs from the same network need to be set on localhost, as the machine will be utilized as both server and client (Rifky The Cyber, 2022).

1. **Location Tracking Attack**

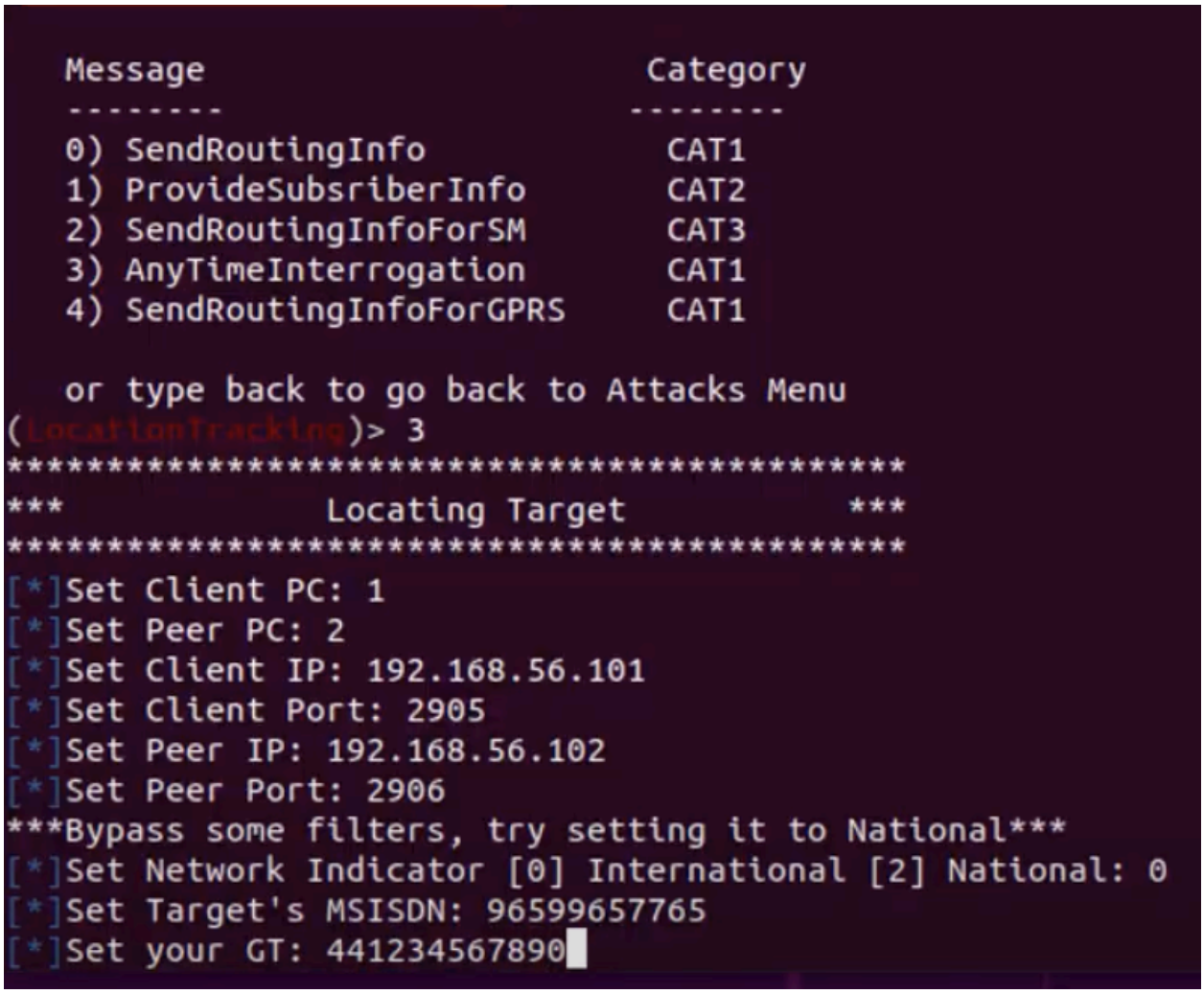


Fig 1. : Location Tracking Attack using AnyTimeInterrogation

Once the attack is launched, Wireshark will be used to capture the location data. The AnyTimeInterrogation is executed to send out a location inquiry, and in response, we will receive a confirmation, specifically a SACK AnyTimeInterrogation, containing the targeted individual's location information (Rifky The Cyber, 2022).

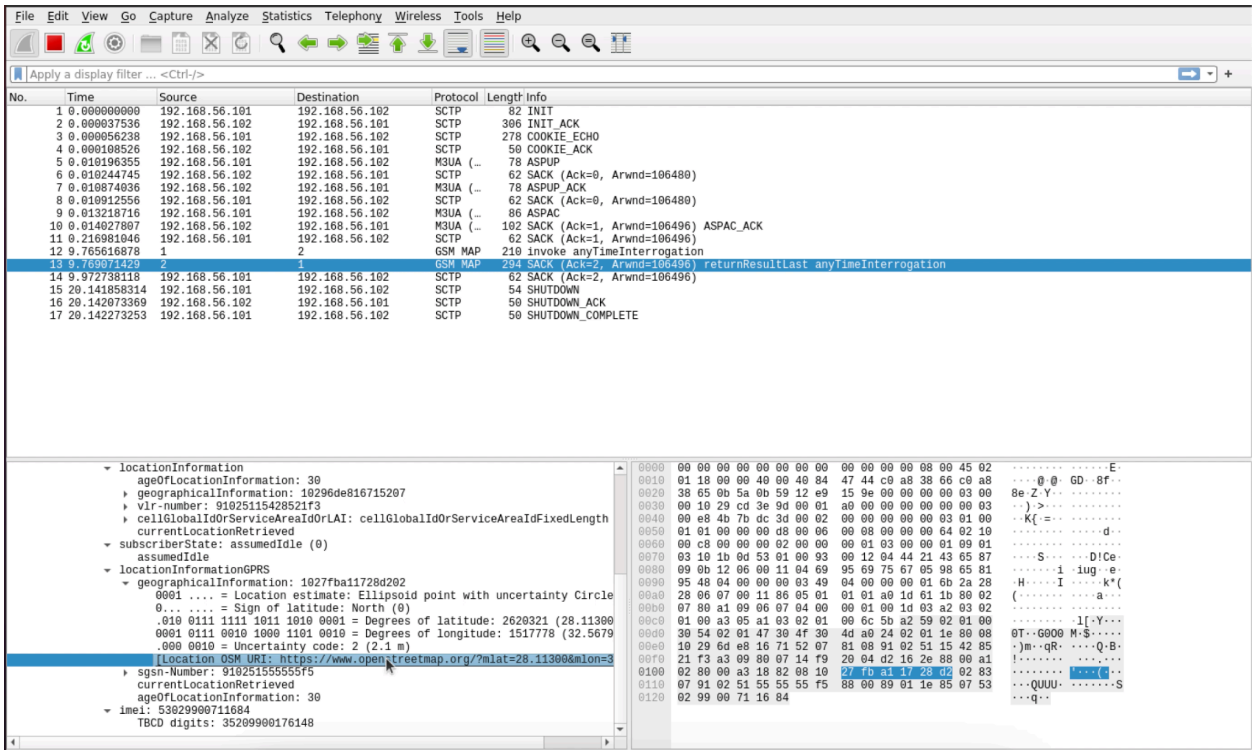


Fig. 2: Captured data in Wireshark

The location information was extracted from the dataset gathered via Wireshark.

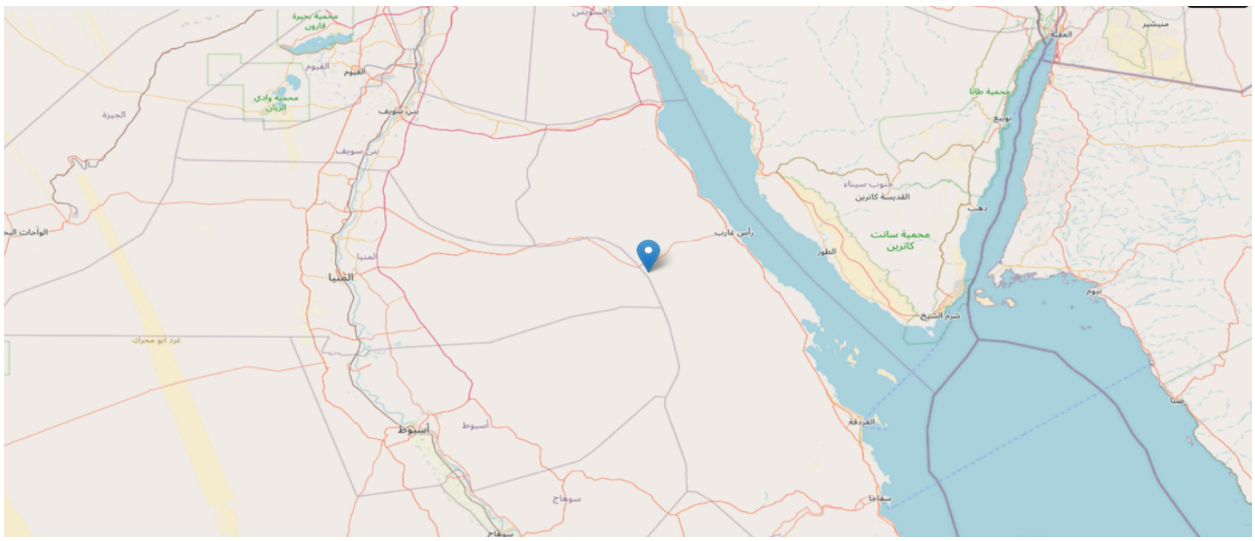
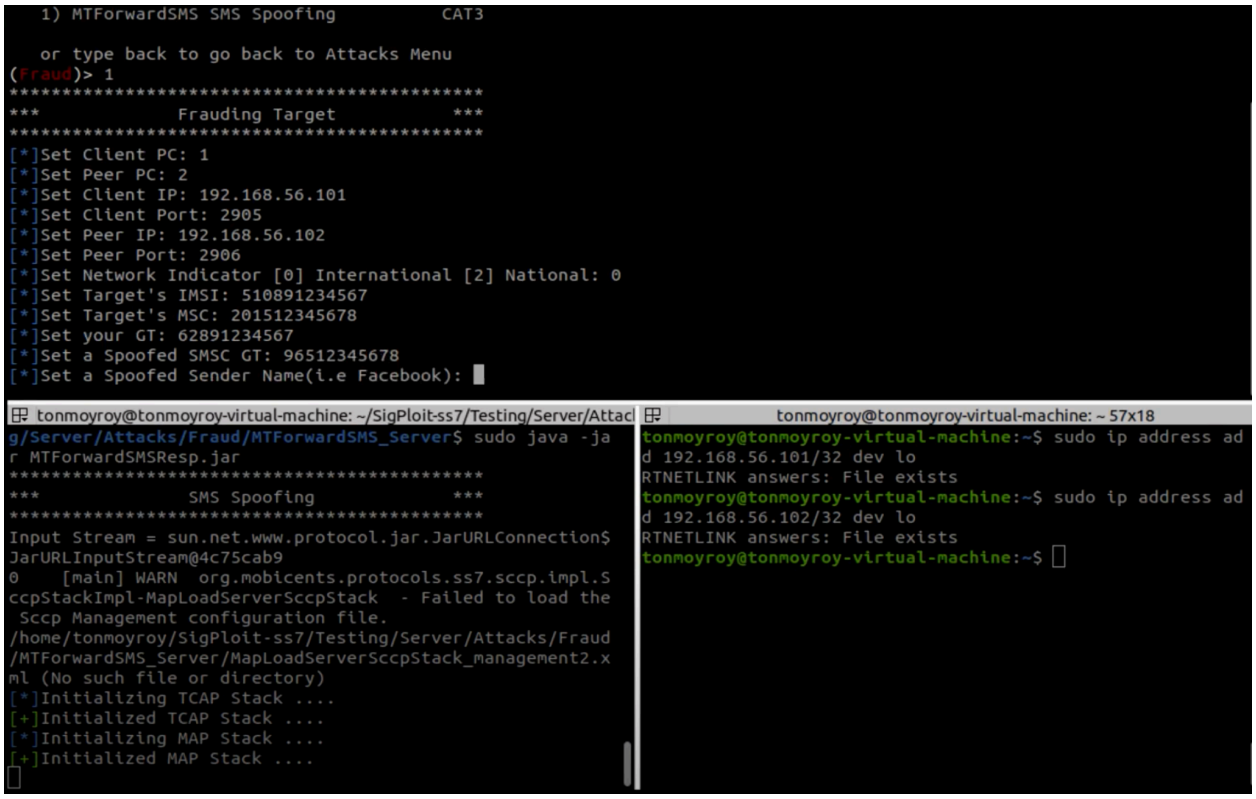


Fig. 3: Target's location using Latitude and Longitude

2. Phishing Mail (Fraud)



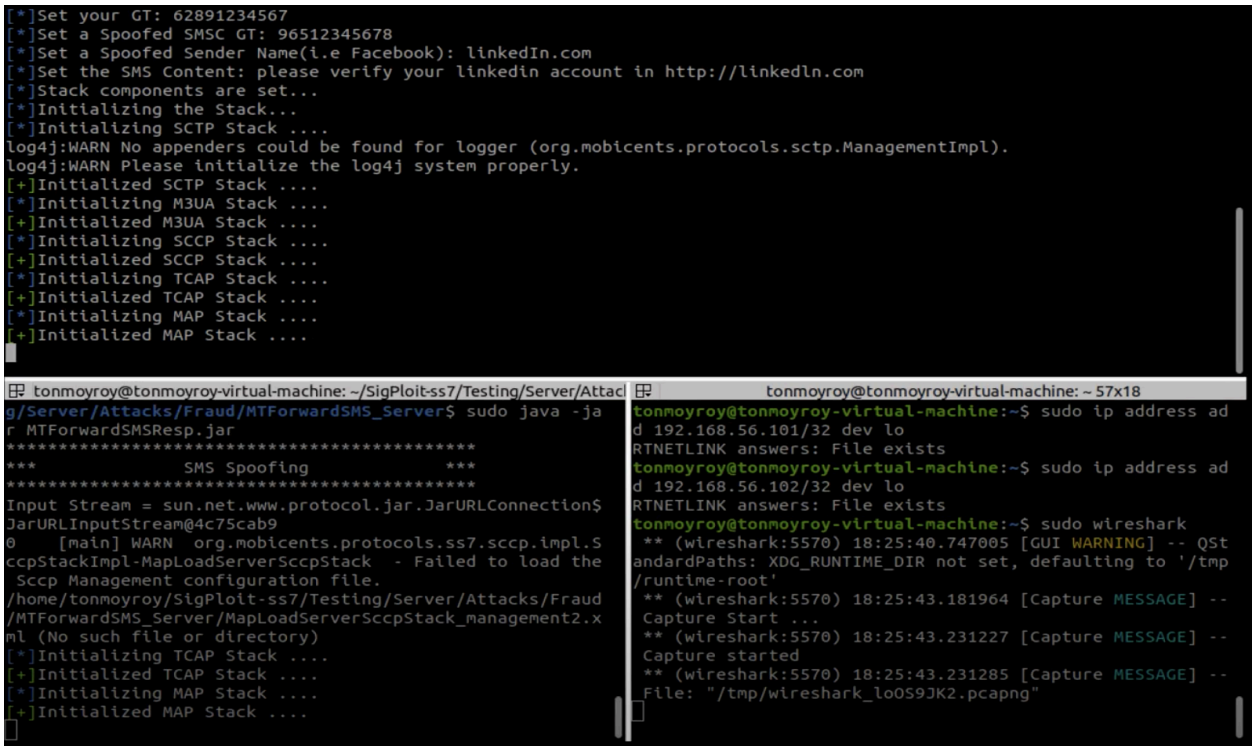


Fig. 4 & 5: Phishing Mail Attack

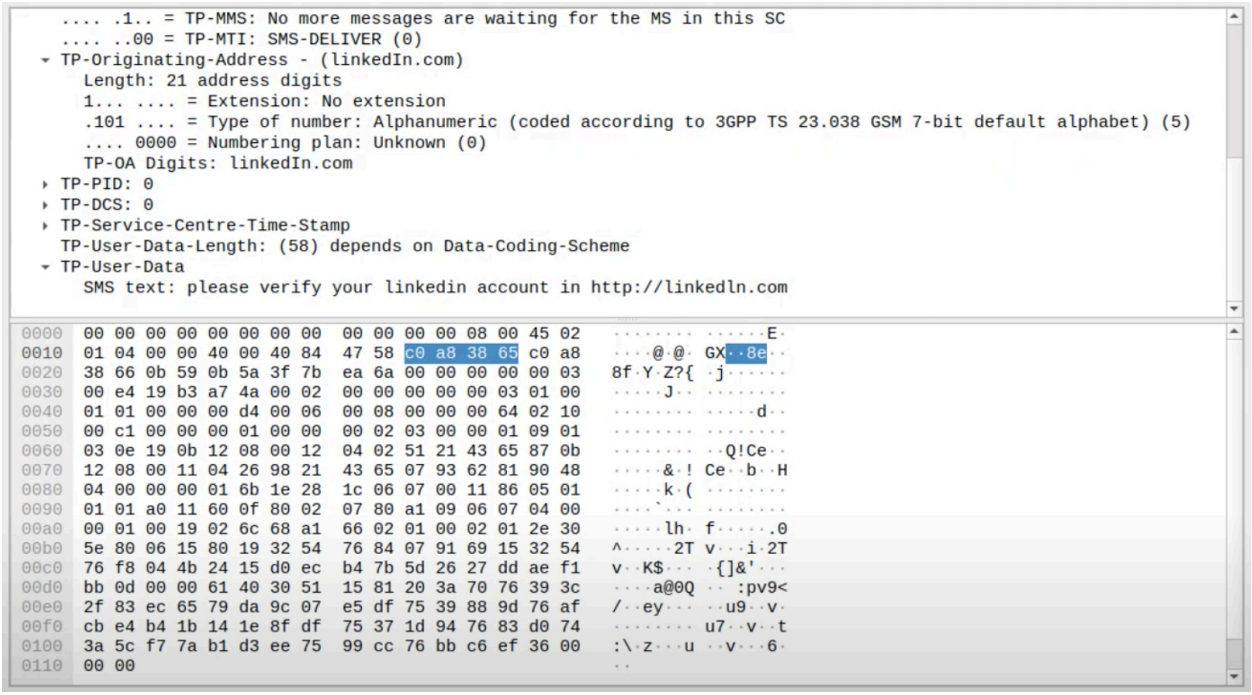


Fig. 6: Output in Wireshark After Attack Initialization

3. SMS Interception

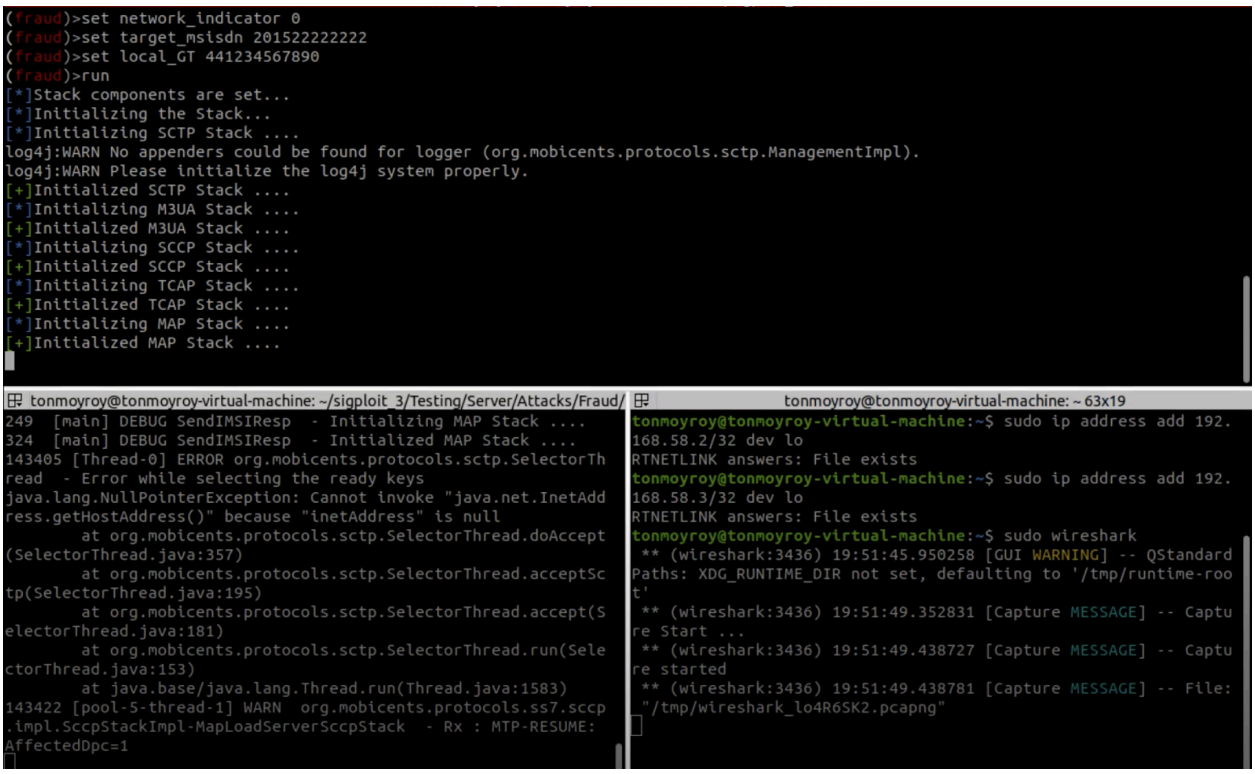


Fig. 7: SMS Interception Attack

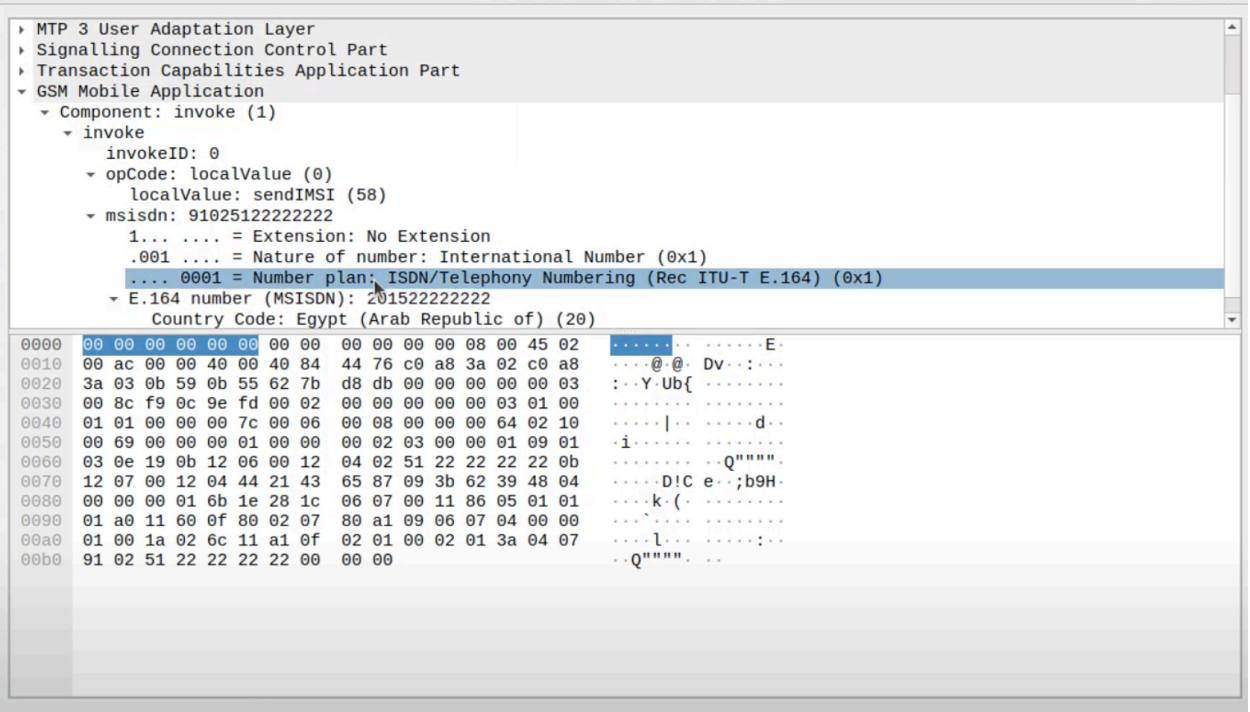


Fig. 8: Output in Wireshark After Attack Initialization

1] Steiner, B., Escoto, L., Sefa, E., & George, J. (2019). Exploring the inherent vulnerabilities in SS7 technology using SigPloit. In *Cysecure.org*. http://cysecure.org/560/online/project/sigploit_brianSteiner_joyGeorge_louisEscoto_emmanuelSefa.pdf

2] Cleary, B. (2020, January 2). *8 SS7 vulnerabilities you need to know about*.Cellusys. https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/?fbclid=IwAR12

3] Mahar, B. (2021, July 7). *3G: Practical attacks against the SS7 signaling Protocol*. Kroll. https://www.kroll.com/en/insights/publications/cyber/3g-practical-attacks-against-the-ss7-signaling-protocol

4] Rifky The Cyber. (2022, September 30). *Part 1: how to trigger SS7 AnytimeInterrogation from our computer* [Video]. YouTube.

https://www.youtube.com/watch?v=-_7_wKhzY2A