

# Forum:[Hack Forums](#)

Thread: [True Blackhat Cellular/Phone Exploitation TTP: Sigsplot for SS7](#)

Tyr - September 29, 2026, 8:15 pm

SigPloit Offensive Guide for Beginners: Learning [SS7 Vector Attacks](#)

What is SigPloit?

SigPloit is a framework designed for SS7 (Signaling System 7) penetration testing. SS7 is the global telecommunications protocol that powers cellular networks, handling call routing, SMS delivery, and subscriber mobility. Despite being decades old, it was designed without security in mind, making it vulnerable to various attacks.

Prerequisites

Knowledge Requirements

Basic understanding of telecommunications concepts is essential before diving into SS7 exploitation. You should also be familiar with the Linux command line, have a solid understanding of networking fundamentals including TCP/IP and protocols, and possess basic Python knowledge for scripting extensions.

System Requirements

You will need a Linux operating system, with Kali Linux being preferred though Ubuntu or Debian are acceptable alternatives. Your hardware should have a minimum of 4GB RAM and 10GB of free disk space. An internet connection is required for downloading dependencies. Most importantly, you need legitimate SS7 network access through a proper MAP or CAP access point.

Installation

To install SigPloit, begin by cloning the repository from GitHub. Navigate to the SigPloit directory once downloaded. Install the required Python dependencies using pip. Make the main script executable and then run it using Python.

SS7 Attack Vectors

Location Tracking is one of the primary attack vectors, allowing you to intercept subscriber location information and track device movement across cell towers without any notification to the target. SMS Interception enables redirecting text messages to the attacker, effectively bypassing end-to-end encryption and capturing two-factor authentication codes. Call Interception allows redirecting voice calls to enable eavesdropping and modify call routing. Denial of Service attacks can block subscriber services, prevent call and SMS delivery, and cause network disruption. USSD Fraud involves triggering premium services remotely to drain victim credit, executed silently without user notification.

/// Practical Usage:

Step 1: Environment Setup

SigPloit requires SS7 network access for testing. You will need a valid Global Title, a Signaling Point Code, and proper SS7 network connectivity.

## Step 2: Select Attack Module

Launch the framework using Python, then select your attack category from the available options including Information Gathering, Location Tracking, Interception, Fraud, or Denial of Service.

## Step 3: Configure Parameters

Each module requires specific parameters to function. You need the target IMSI, which is the International Mobile Subscriber Identity. The target MSISDN in E.164 format including the country code. The target VLR address representing the Visitor Location Register. And the target HLR address representing the Home Location Register.

## Step 4: Execute Attack

For example, when executing a Location Tracking attack, select module 2, enter the target IMSI such as 310150123456789, enter the target MSC or VLR Global Title like 123456789012, enter your own Global Title, and execute the attack.

## Key Modules Explained

Location Tracking using AnyTimeInterrogation allows you to retrieve cell tower location using the IMSI and VLR address as parameters, outputting the Cell ID, Location Area Code, and precise geolocation. SMS Interception redirects SMS to the attacker using UpdateSMSRouting with your Global Title, requiring proper MAP dialogue establishment. Call Forwarding redirects incoming calls using InsertSubscriberData with a modified Forwarded-To Number, persisting until removed or until timeout. USSD Push executes USSD codes remotely for premium service activation or balance queries, delivering silently without user notification.

## Advanced Techniques

Custom Message Crafting allows for non-standard attacks by building custom MAP or CAP messages using Python libraries like Scapy. You can construct messages with specific IMSI and Global Title values and send them via SCTP or M3UA protocols.

GT Spoofing involves Global Title spoofing to impersonate other operators, bypass basic filtering mechanisms, though this requires access to valid Global Title range assignments.

Multi-Hop Attacks involve chaining multiple SS7 nodes to obscure your origin, beginning at a partner network entry point, transiting through an international exchange, targeting the destination network, and returning through a reverse response path.

## Detection Evasion

Timing Controls help evade detection by spacing requests to avoid rate limiting, mimicking legitimate traffic patterns, and randomizing request intervals. GT Rotation involves using multiple Global Titles, rotating through legitimate ranges, and avoiding repeated source addresses. Protocol Compliance requires maintaining proper SCCP and TCAP state, using valid Application Contexts, and following MAP dialogue rules precisely.

## Defensive Countermeasures

Understanding defenses helps bypass them effectively. Filtering Systems include GT Blacklisting which can be countered by rotating GTs, Message Screening which requires crafting valid-looking messages, Rate Limiting which can be bypassed by implementing delays, and SCCP Whitelisting which requires using whitelisted GT ranges. Modern Defenses include SIGTRAN Security using IPsec and TLS, Diameter Edge Agents for protocol translation, AI-Based Detection using behavioral analysis, and SS7 Firewalls performing deep packet inspection.

## Legal and Ethical Framework

Authorized Testing Only requires written permission from the network operator, explicitly defined scope for targets, scheduled maintenance windows for timing, and full disclosure of all findings. Illegal Activities include testing without authorization, intercepting real subscriber data, disrupting commercial services, and selling vulnerabilities or exploits. Responsible Disclosure requires documenting findings, reporting to the affected operator, allowing time for remediation, and only pursuing public disclosure after fixes are implemented.

## Troubleshooting

Common Issues include Connection Refused errors which require verifying SIGTRAN connectivity, checking firewall rules, and confirming the SCTP port typically 2905. Dialogue Rejected errors indicate invalid Application Context, version mismatch, or missing mandatory parameters. Provider Abort errors stem from SCCP routing failure, GT translation errors, or network congestion.

Debug Mode can be enabled using verbose logging flags. Packet capture can be performed using tcpdump on the appropriate network interface saving to a file with SCTP port 2905 filtering, then analyzed using Wireshark.

## Resources and References

Key documentation includes 3GPP Specifications TS 29.002 for MAP and TS 29.078 for CAP. ITU-T Standards in the Q.700 series cover the SS7 protocol stack. SIGTRAN is documented in RFC 2719 and RFC 3286. Security research can be found in CCC and Black Hat SS7 presentations. (<https://attack.mitre.org/detectionstrategies/DET0662/>) (<https://www.p1sec.com/blog/legacy-and-modern-protocols-at-risk-ss7-diameter-gtp-ims-5g-security-threats>) (<https://fight.mitre.org/techniques/FGT1071.502/>)

Legal Disclaimer: I am not responsible for your actions and all information provided here is for educational purposes only with the intent to train people on offensive hacking. Many of these tools require expertise with Kali Linux and should be used only ethically and in a legal environment.

## Goals and TTP:

With SS7 exploitation through tools like SigPloit, an attacker with network access can accomplish several serious attacks against cellular subscribers:

### Surveillance and Tracking

Track someone's physical location in real time without their knowledge by querying which cell tower their device is connected to. This works globally and can pinpoint a target within a few hundred meters in urban areas. Intelligence agencies and law enforcement have used this to track persons

of interest across borders without local cooperation.

#### Communications Interception

Intercept text messages and phone calls before they reach the intended recipient. This includes capturing two-factor authentication codes sent via SMS, allowing account takeovers for banking, email, social media, and cryptocurrency exchanges. Voice calls can be redirected to attacker-controlled numbers for eavesdropping.

#### Financial Fraud

Execute USSD codes that transfer money, check balances, or activate premium services that drain victim accounts. Some attacks can redirect mobile banking confirmations or payment authorizations. In regions where mobile money is prevalent, this enables direct theft.

#### Denial of Service

Prevent a target from receiving calls or texts by blocking their IMSI registration or redirecting all their traffic to a dead end. This can be used to prevent someone from calling for help, receiving security alerts, or maintaining business communications.

#### Account Takeover

Combined with social engineering or credential stuffing, SMS interception allows bypassing 2FA on virtually any platform that uses SMS verification including Gmail, WhatsApp, Telegram, banking apps, and cryptocurrency wallets.

#### Real World Impact

In practice, these capabilities have been used by nation-states to track political dissidents, by criminal groups to empty bank accounts, by stalkers to monitor victims, and by intelligence agencies to bypass wiretap requirements. The SS7 network's lack of authentication means attacks can originate from compromised or rogue telecom operators anywhere in the world and affect subscribers globally.

#### Who Actually Uses This

Beyond security researchers testing their own networks, these techniques are actively used by advanced persistent threat groups, organized crime syndicates with telecom access, nation-state intelligence services, and in some cases corrupt insiders at telecommunication companies.

The knowledge also serves defensive purposes. Understanding these attacks helps security engineers design monitoring systems, implement SS7 firewalls, and transition to more secure protocols like Diameter with proper edge security.

#### Conclusion

SS7 exploitation remains relevant as long as legacy networks persist. SigPloit provides a framework for understanding these vulnerabilities, but requires legitimate network access and proper authorization. The knowledge gained from studying these attacks helps in designing more secure next-generation networks using Diameter and HTTP/2 based 5G core architectures.

#### Sources

<https://citizenlab.ca/research/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>  
[https://www.3gpp.org/ftp/tsg\\_sa/wg3\\_security/specs/33900-120.pdf](https://www.3gpp.org/ftp/tsg_sa/wg3_security/specs/33900-120.pdf)  
<https://www.youtube.com/watch?v=ecmnOllr25Q>

<https://firecompass.com/exploiting-ss7-vulnerabilities-sigploit/>

Remember that with great power comes great responsibility. This knowledge should only be used for authorized security testing and educational purposes.

## Sources

**Lowkey** - September 30, 2026, 3:59 am

Wow, a real thread. Thank you you Tyr, good read.

**Tyr** - September 30, 2026, 12:11 pm

(Sep 30, 2026 03:59 AM)Lowkey Wrote: [\[CITE\]](#) Wow, a real thread. Thank you you Tyr, good read. You're welcome my friend. Hope everyone can benefit ethically and learn together from this.

**Sift** - October 1, 2026, 5:12 am

High quality thread, well written and straight to the point.