Copper Strand Substrate Intrusion (CSSI)

Author: **William J. Appleton**
Date: May 2025
Category: Anti-Forensic Research / Hardware Subversion
Version: 1.0

Abstract

This paper introduces Copper Strand Substrate Intrusion (CSSI), a novel anti-forensic technique designed to neutralize forensic recovery attempts on NAND-based solid-state storage (e.g., NVMe SSDs) by embedding micro-conductive elements within the BGA substrate zone of flash memory packages.
The technique enables full device functionality under normal operating conditions while posing a high likelihood of catastrophic failure under forensic-level probing, particularly during bit-level imaging or chip-off extraction. CSSI is designed to operate as a passive, self-defeating sabotage mechanism against physical and logical data recovery attempts.

1. Introduction

Traditional forensic countermeasures on solid-state drives (SSDs) involve software-level sanitization (e.g., overwriting data, ATA secure erase) or physical destruction. However, forensic imaging tools continue to evolve, allowing partial recovery of metadata and raw flash dumps even after standard wiping techniques. In response, the CSSI technique introduces a stealth, non-destructive, hardware-level contingency that:

- Allows plausible operational integrity at time of inspection,
- Remains undetected during standard visual or software examination,
- Creates a latent fault condition that activates during advanced forensic activity.

2. Technical Background

Modern NAND flash memory packages, particularly those utilizing BGA (Ball Grid Array) packaging, interface with the host system via dense arrays of micro-soldered balls. These balls carry signal lines for:

- Power (Vcc, VccQ)
- Ground (GND)
- Command and address lines (CE#, ALE, CLE)
- Data (DQ0–DQ7)
- Control signals (WP#, R/B#)

Advanced forensics may attempt bit-level imaging or even chip-off techniques to recover overwritten or hidden data by accessing raw NAND. CSSI aims to sabotage these efforts without degrading normal system use.

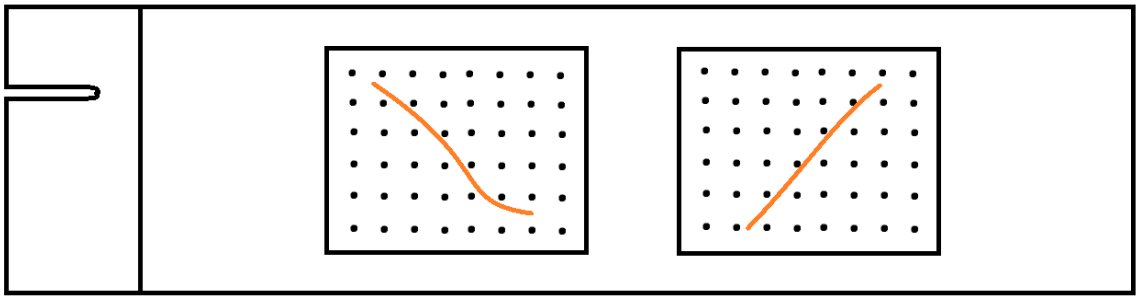
3. Method: Copper Strand Substrate Intrusion (CSSI)

3.1 Materials and Setup

- Conductive element: A single, uninsulated copper strand (extracted from a standard USB cable), ~6–8 mm in length, ~50–100 µm diameter
- Target: BGA NAND flash packages on NVMe SSDs
- Tools: Fine-tipped non-conductive tweezers, magnification, isopropyl alcohol for final cleaning

3.2 Procedure

1. After securely wiping the SSD (e.g., via dd), the NAND packages are targeted.
2. A copper strand is carefully inserted laterally into the gap beneath the NAND BGA package.
3. The strand is inserted such that:
   - It is no longer visible even with magnified inspection and directed light.
   - It spans ~70% of the chip width, potentially contacting or floating near multiple solder balls.
4. The drive is cleaned with alcohol and reassembled.



3.3 Behavioral Profile

Condition	Observed Behavior
Normal system boot	Fully operational
Read/write cycles	Stable
Imaging or chip interrogation	High risk of drive failure or data corruption

4. Activation Mechanism

The CSSI strand acts as a latent shorting bridge or high-impedance path between solder balls. It remains electrically inert during typical use due to:

- Low signal stress
- Controlled thermal expansion

However, during forensic activities such as:

- Full-disk imaging
- Rapid, sustained NAND access
- Chip heating during desoldering or X-ray

…the following can occur:

- Thermal drift moves the strand into new positions
- Voltage differentials create unintended shorts
- Electromigration or arcing corrupts adjacent lines

This results in:

- Bit errors
- Bus conflicts
- Permanent controller lockup
- Total loss of flash access

5. Detection and Forensic Countermeasures

5.1 Detection Challenges

- CSSI is invisible to standard diagnostics
- Does not impact SMART data or POST tests
- Evades detection unless non-destructive imaging (X-ray, acoustic microscopy) is used

5.2 Forensic Risk

If an analyst attempts chip-off recovery or uses high-frequency signal probing:

- The strand may cause unrecoverable chip or controller failure
- NAND reads may become corrupted or result in inconsistent dumps
- Recovery efforts may destroy remaining viable data, acting as a self-destruct

6. Conclusion

CSSI represents a sophisticated passive anti-forensic measure leveraging physical intrusion at the substrate level. Unlike encryption or overwriting, it provides destructive fail-safe behavior only when advanced forensic analysis is attempted, thereby functioning as a conditional deterrent. It is especially effective against forensic teams lacking hardware inspection capabilities and relies on stealth, subtlety, and hardware behavior under stress.

7. Future Research

- Use of non-metallic conductive composites to further reduce detectability
- Application to other chip types (e.g., eMMC, DRAM, microcontrollers)
- Controlled development of time-delayed shorts using temperature-sensitive elements

****Disclaimer:** *This document is a theoretical exploration for academic and technical discussion only. It does not advocate real-world implementation of destructive techniques against electronic property.***