



# SIGINT FORENSICS CENTER

(S//REL) *Tracking Courier Use of  
Secure Digital Cards*

SIGDEV Conference 2012  
The overall classification of this briefing is:

**TOP SECRET//COMINT//REL FVEY**

Derived From: NSA/CSSM 1-52 Dated: 20070108 Declassify On: 20320108

# (U//FOUO) SD Cards

(U//FOUO) Small

(U//FOUO) Convenient

(U//FOUO) Common

(S//REL) Used by targets



# (S//REL) Tracking SD Cards: The

## Problem

(U//FOUO) No USB Controller

(U//FOUO) FAT Filesystem



(S//REL) The solution: Volume Identification

(U//FOUO) VSN: Volume Serial Number

(U//FOUO) VL: Volume Label

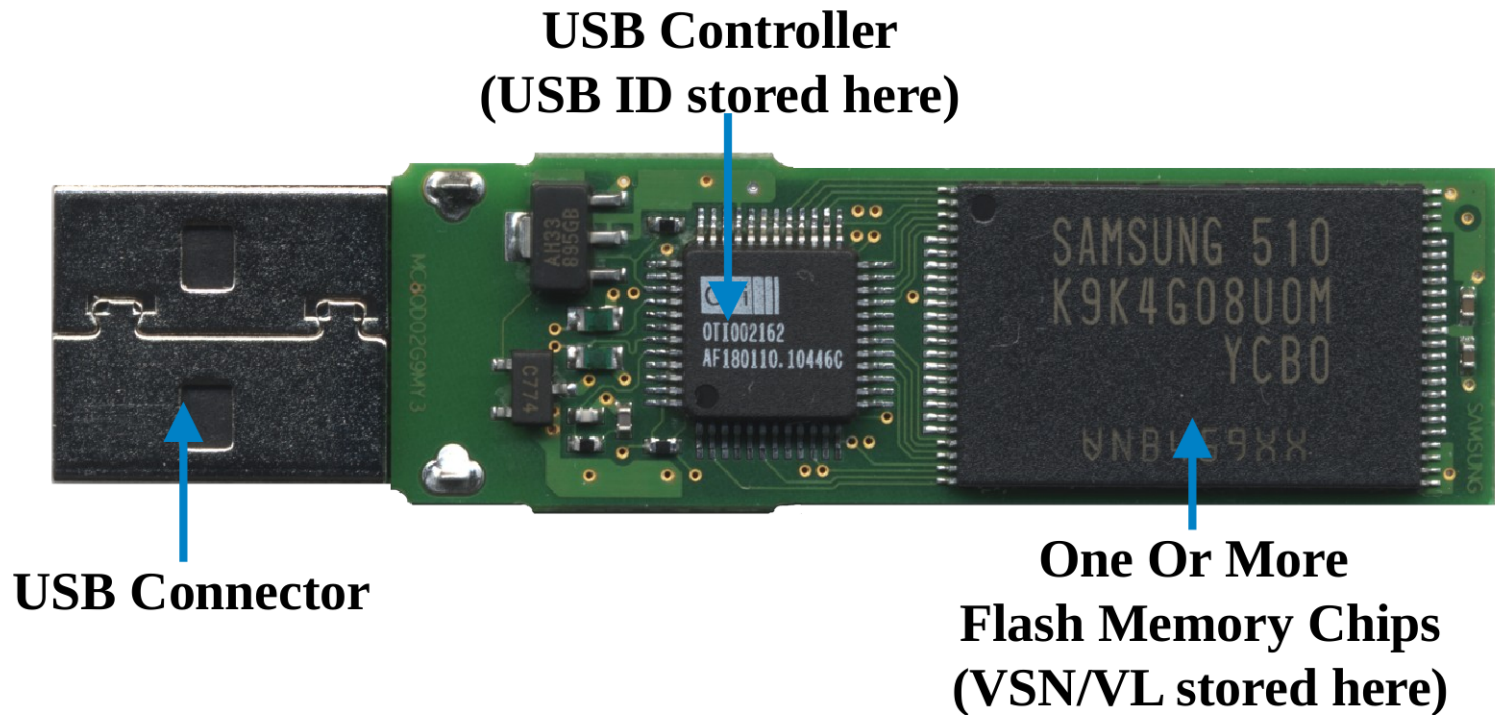
**Actual Values:**

Usama	728c0200
Nokia N73	a7bec691
Google_earth	65ba457d

*Located in the boot sector of a volume*

*\*CDs and DVDs also contain VSN/VLs*

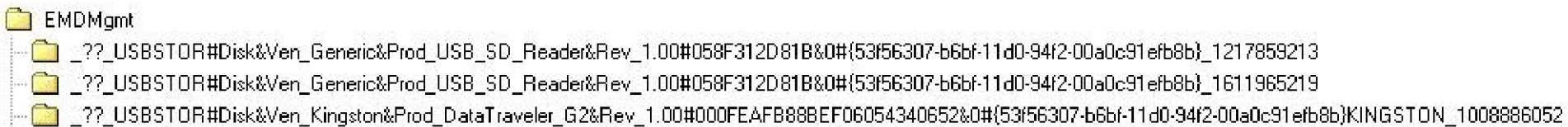
# (S//REL) Unique USB Identification





## (S//REL) VSN/VL Sources

- (S//REL) Filesystem/Volume boot sector
- (S//REL) Windows Registry
  - (S//REL) Vista/7 provide comprehensive history



- (S//REL) XP provides VSN for “last mounted”
- (S//REL) LNK files
  - (S//REL) Identify VSN/VL, device type (CD, removable media, etc)



## (S//REL) VSN/VLs & UBL

(S//REL) Published report (S/OO/SFC/3-12)

(S//REL) Identification information identified for  
36 devices not seized during UBL raid  
16 Missing devices

6 Connected via SD Reader

5 via USB

5 unknown

(S//REL) Determined uniqueness & first  
connect date



# (U//FOUO) Developing a Solution

(TS//SI//REL)



(TS//SI//REL) ***Automated solutions between seized media & CNE media via JOLLYROGER***

(TS//SI//REL)





(U//FOUO) Questions?

# NSA SIGINT Forensics Center



**“GO SFC”**