Controlling USB Flash Drive Controllers:

Exposé of hidden features

Richard Harman

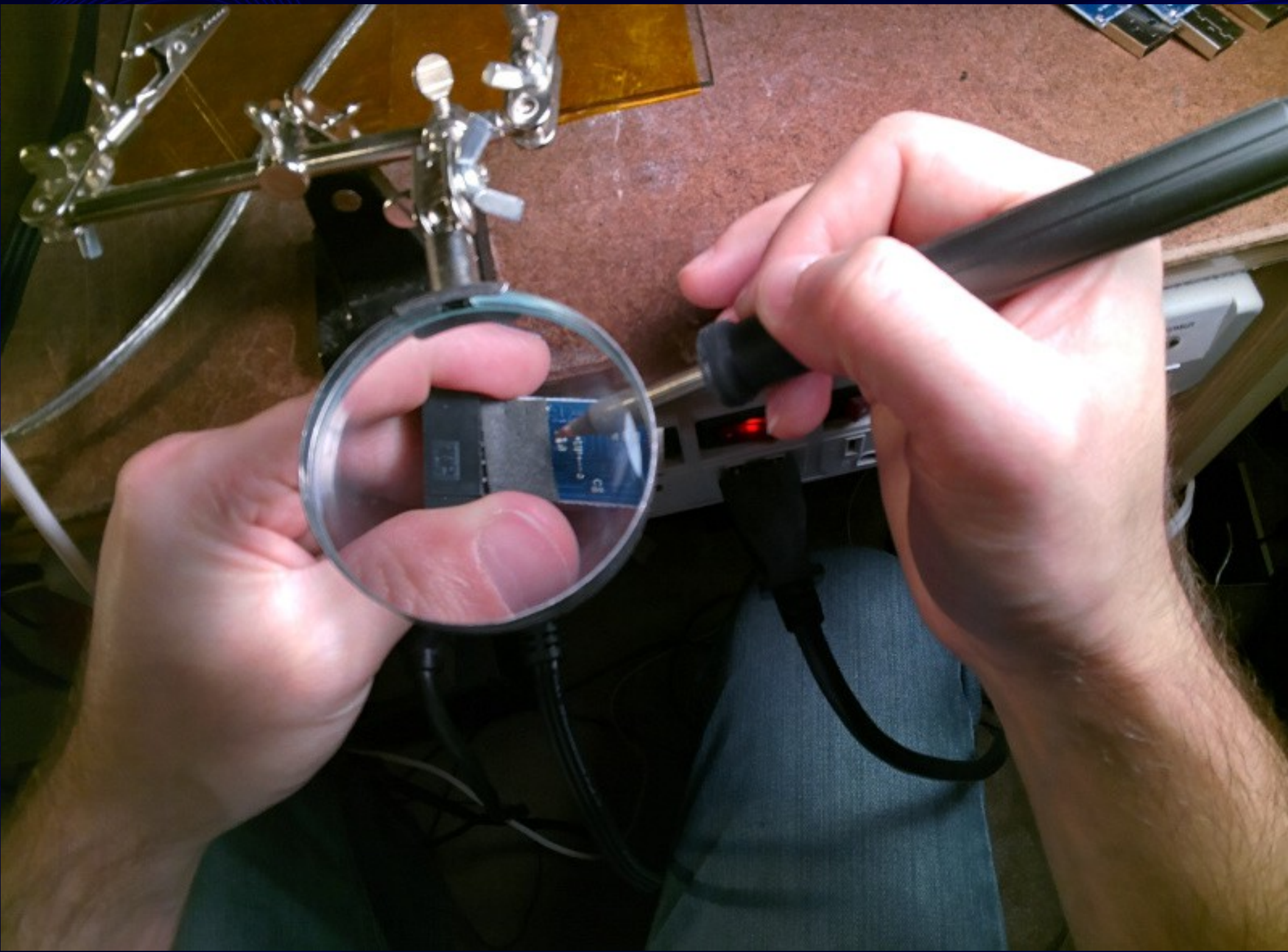
Shmoocon 2014

Richard Harman

- InfoSec Analyst for ~10 years
- Lead Intrusion Analyst at SRA SOC
  - Malware analysis
  - Perl scripting
  - Incident Response & all around SysAdmin-fu

@xabean    warewolf

Richard@RichardHarman.com



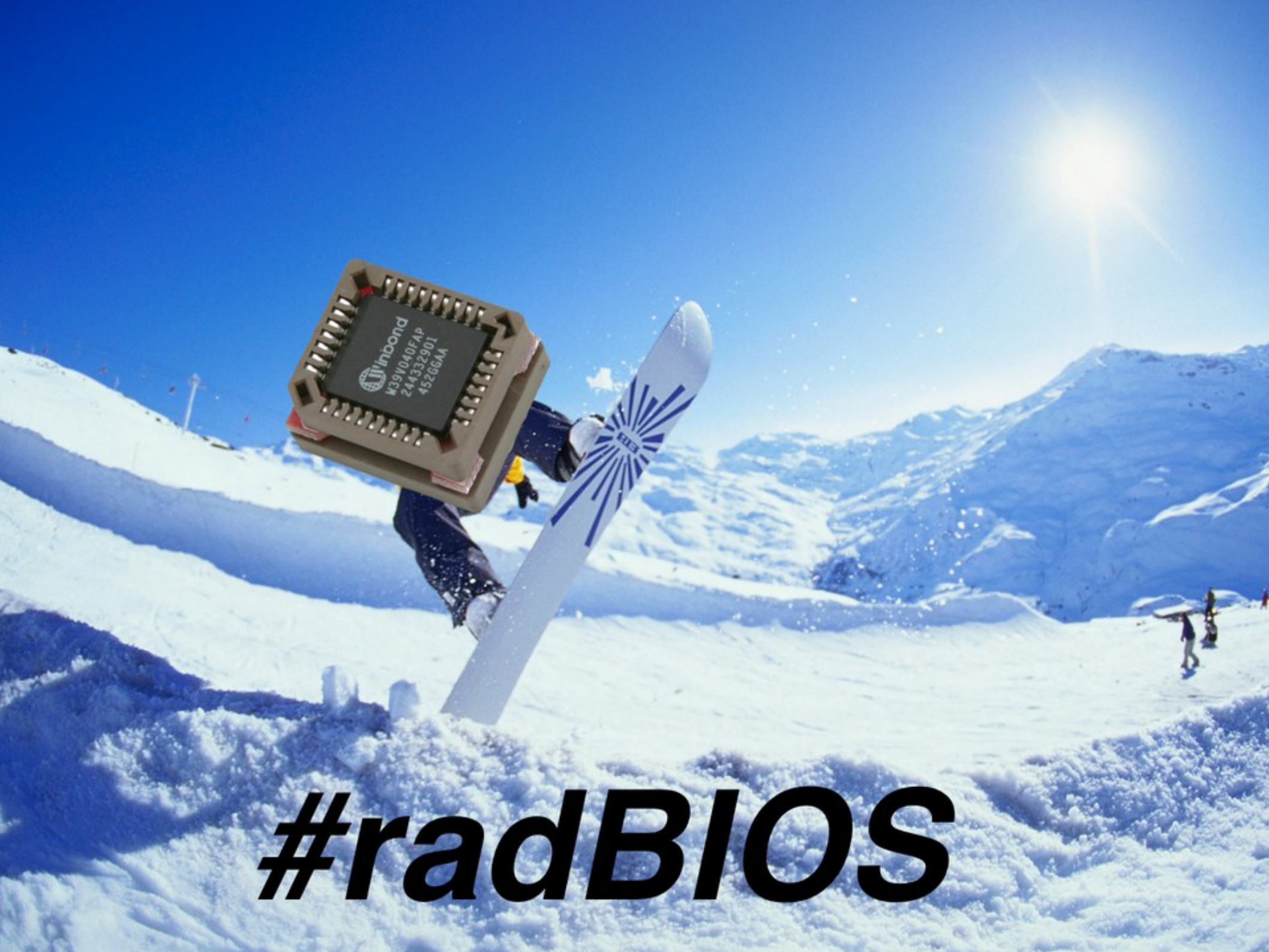

HACKERS


NOVA
Labs

Hacking USB thumb drives


I WANT TO
BELIEVE


#radBIOS


Winbond
W39V040FAP
2443325901
4526GAA
#radBIOS

WORM GENERATOR TOOL V.1.8

HACKSTADY

6548 0548 375 570379821530 126
4625 0558 356 218097534015 156
7890 6207 386 173500783501 169

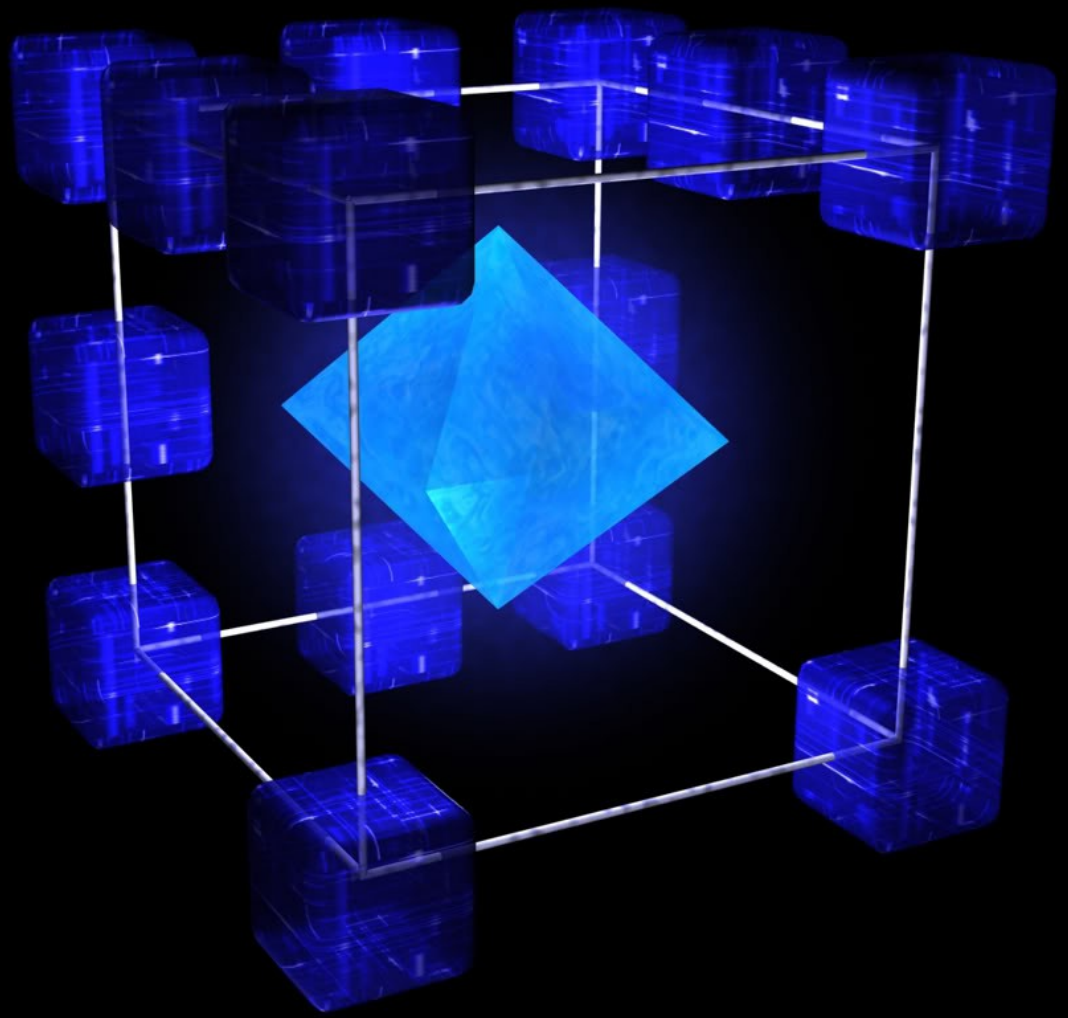
ACCT#: 2657898459:548376
ACCT#: 3759545233:343752
ACCT#: 4568789445:254373

processing.....

4560 9485 9875 2135 7895 4798 7315
9875 6542 9975 2458 4532 2187 7862

- 11D0
- 250D
- 2693
- 857
- 1ED7
- 12BE
- 1C93
- 2693
- 198E
- 26F7
- 99A
- 11B4
- 88B
- 1EB6

ASSEMBLING CRYPTO ALGORHYTHM




#BadBIOS

#BadBIOS ... features ?

1) Spread via USB flash drives
2) Infect USB flash drive firmware
3) Infect host firmware
4) Cross-platform
5) Cross-operating system
6) IPv6 networking
7) Audio-based communication for bridging air-gaps

What?

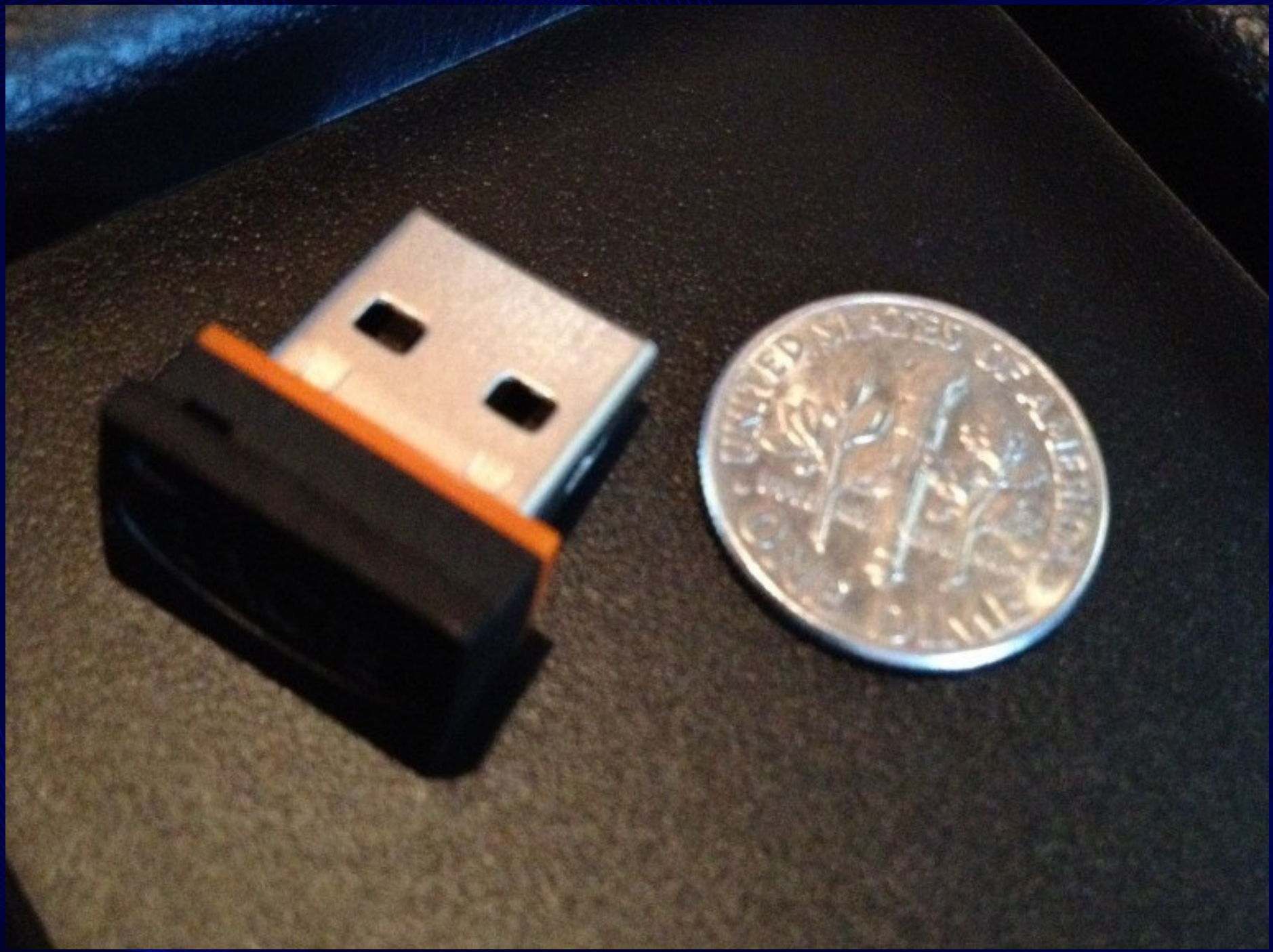
Overview

- USB mass storage hardware
- Hardware Disassembly
- Block-level Components
- Flash Controller Identification & Their Features
- Reprogramming Flash Controllers

USB Mass Storage


Seagate

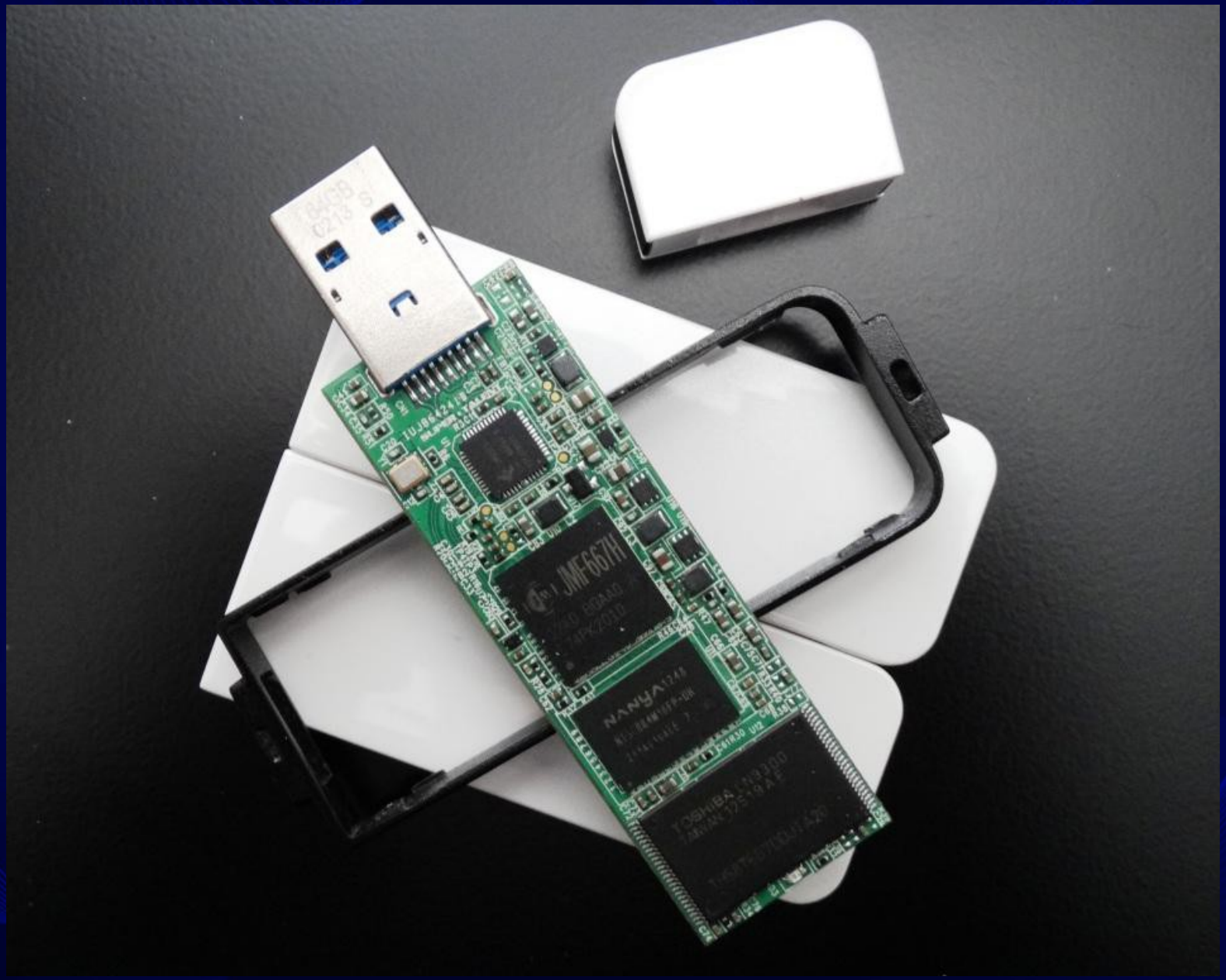

PNY
8GB



Data, Power, controller board, IDE HDD

2.5”, SATA, controller board

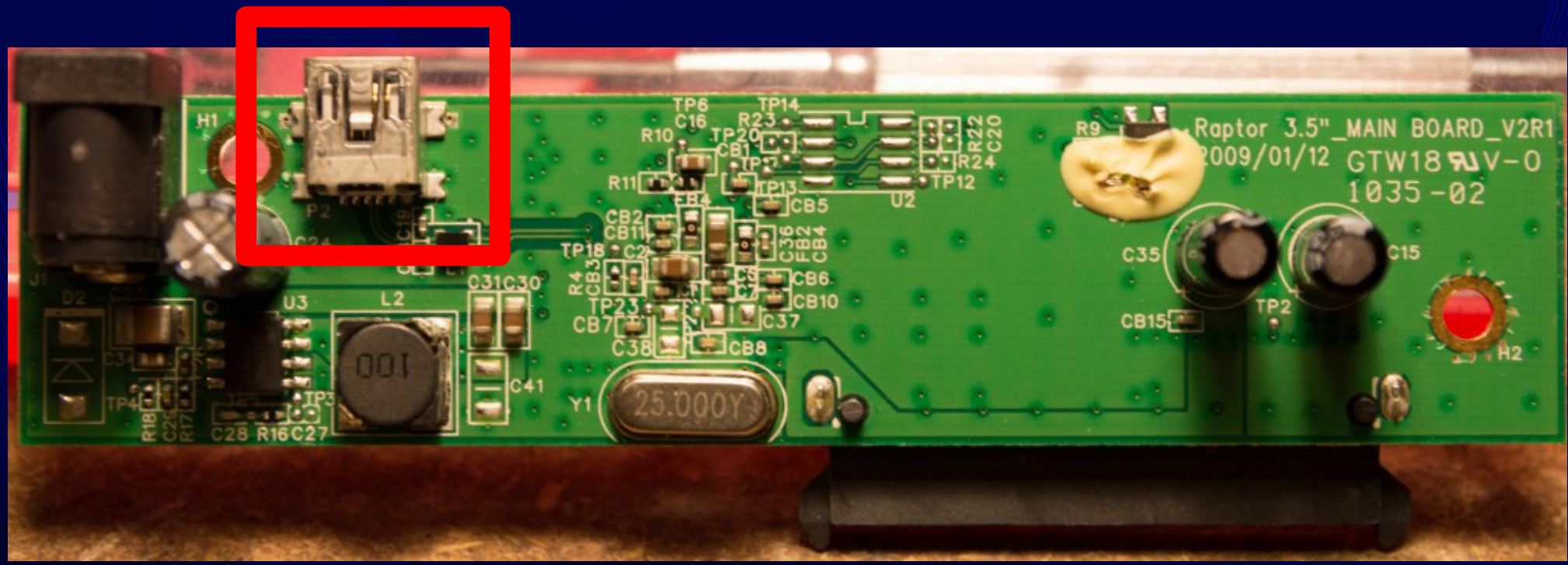
USB3 flash drive



USB HDD
basic components

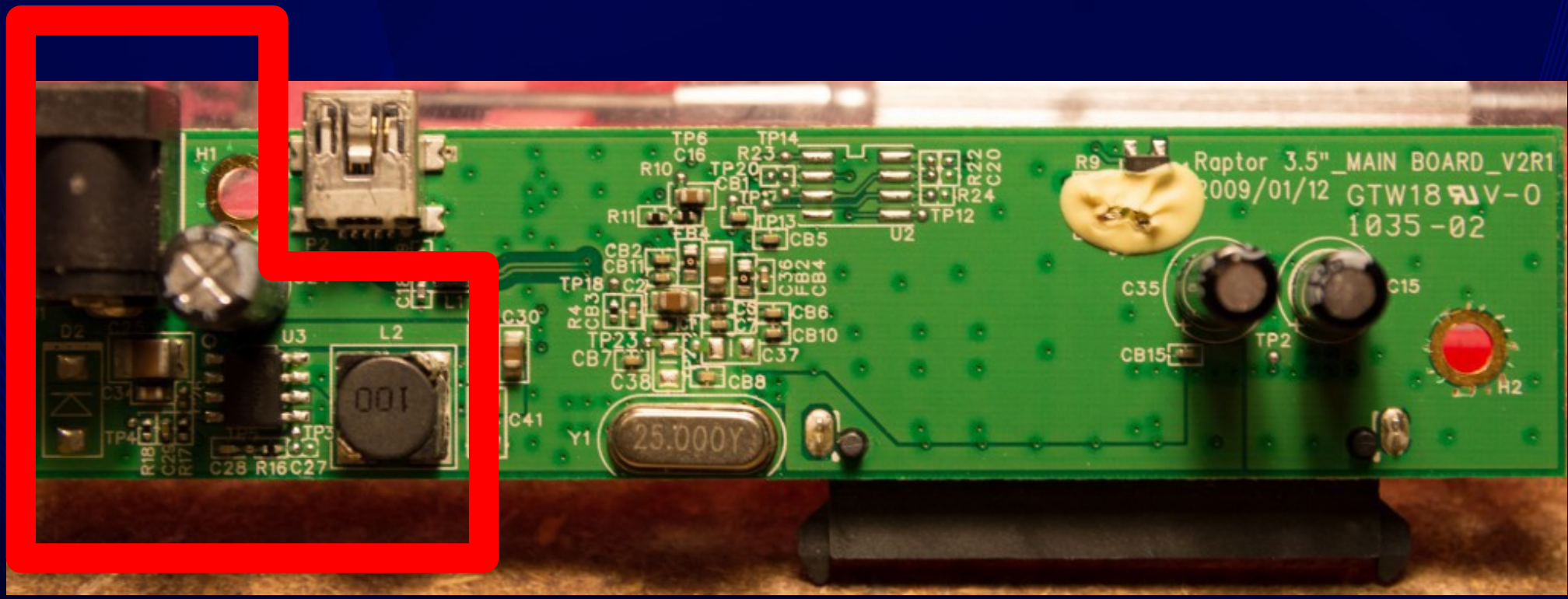
USB SATA HDD Controller/Power board

- Host Interface
- Power



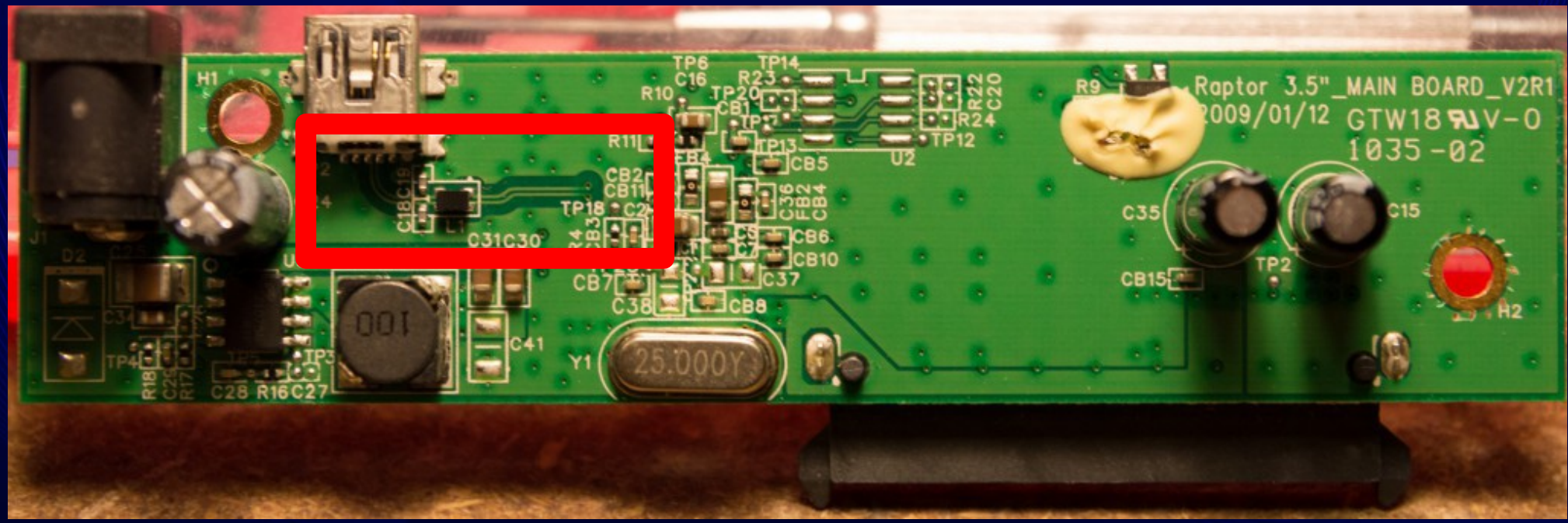
USB SATA HDD Controller/Power board

- Host Interface
- Power



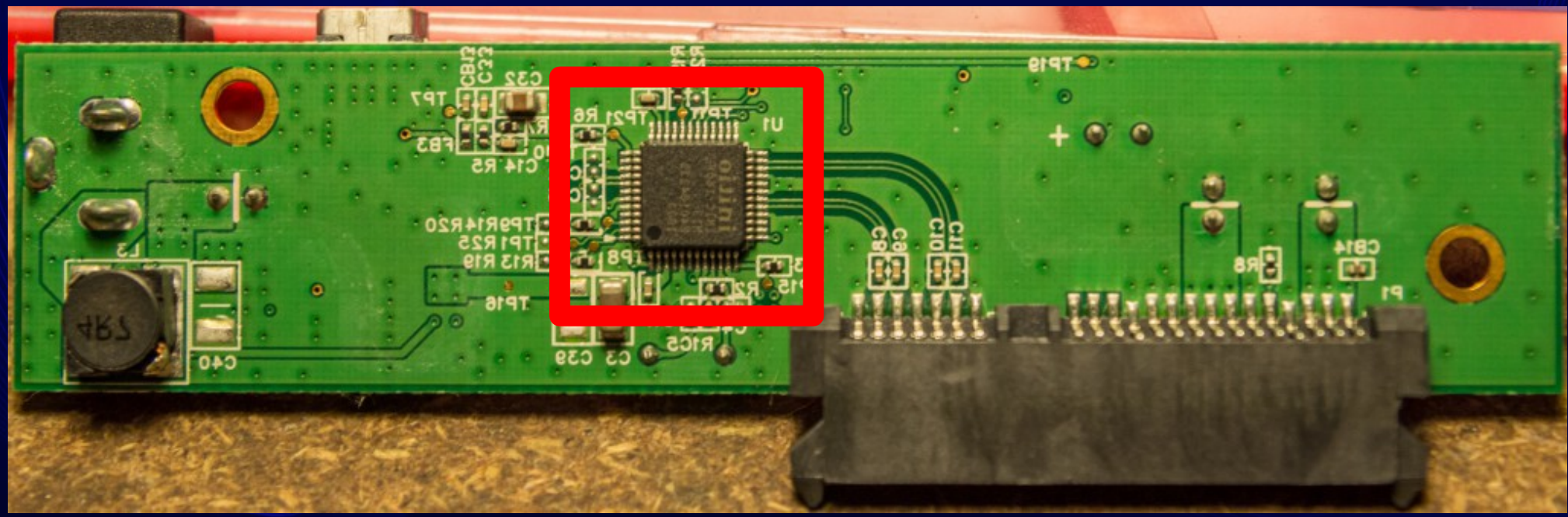
USB SATA HDD Controller/Power board

- USB differential signaling pins



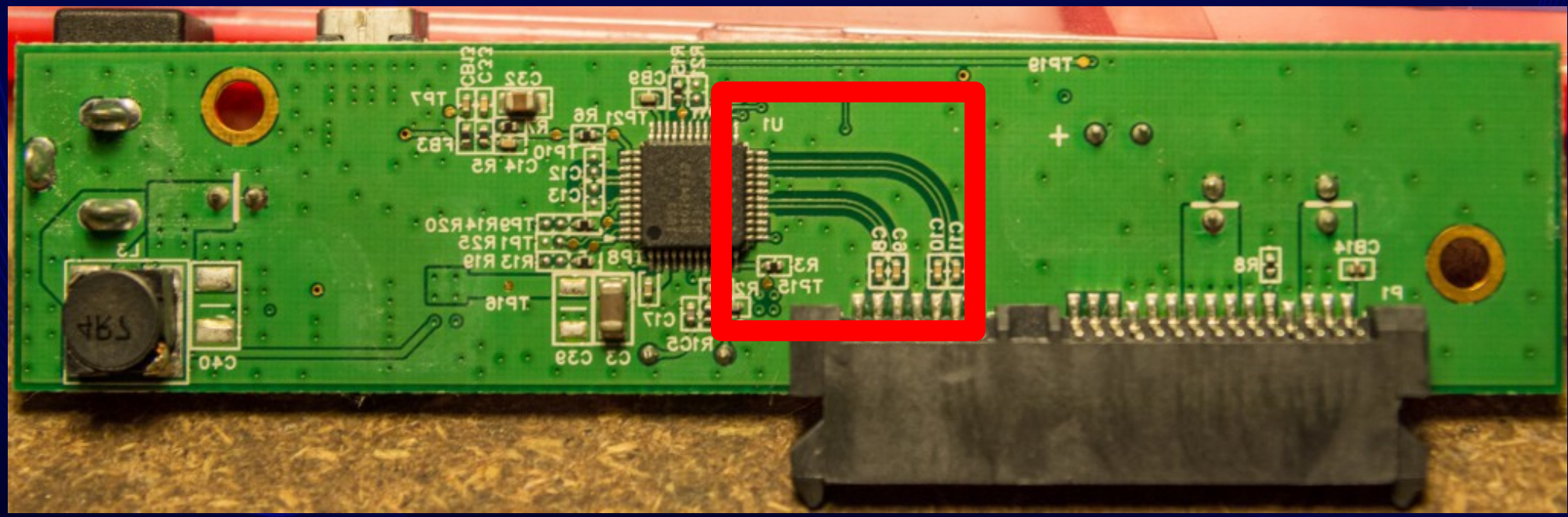
USB SATA HDD Controller/Power board

- Device Interface
- Bridge/Controller



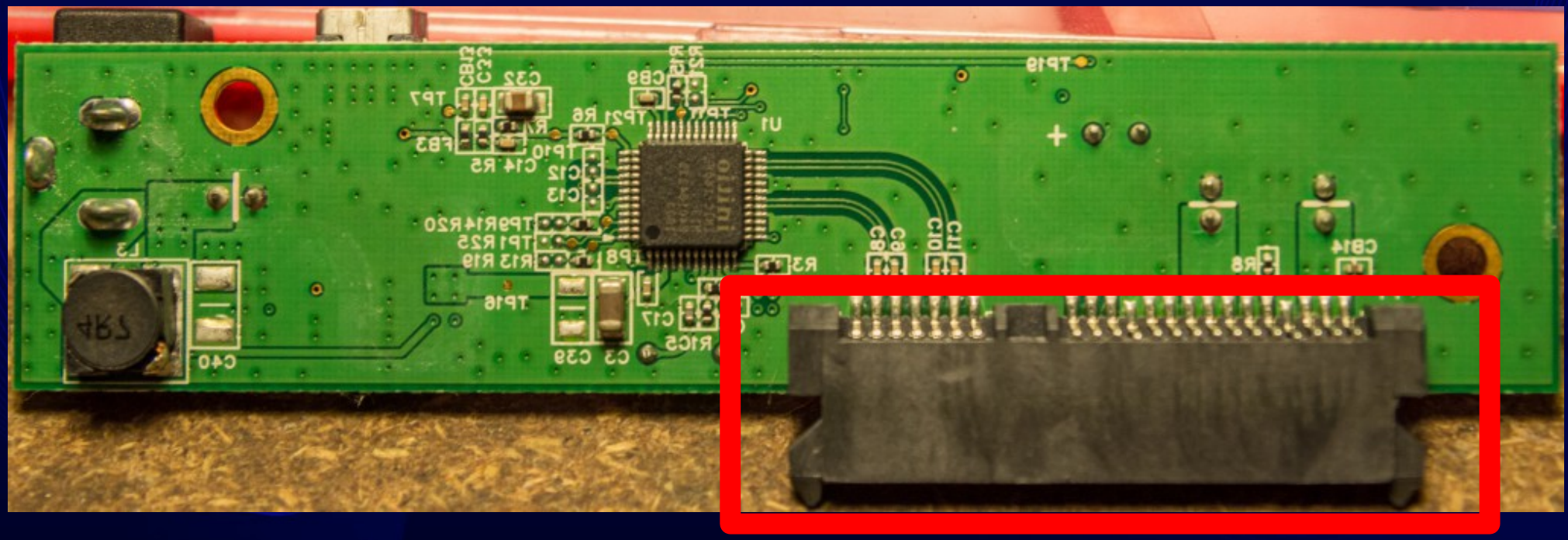
USB SATA HDD
Controller/Power board

- SATA differential signaling pins (2 pair)



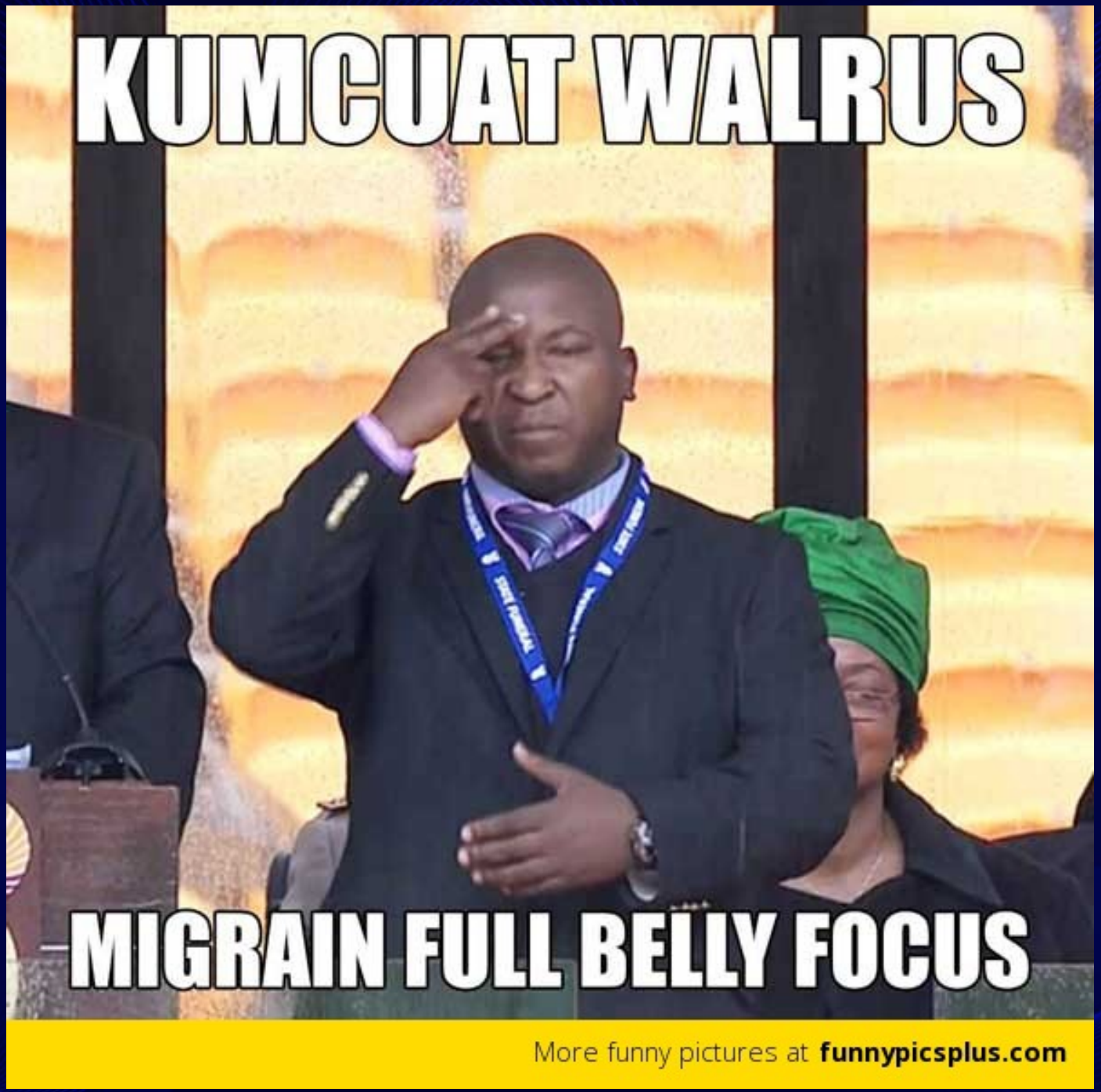
USB SATA HDD Controller/Power board

- Device Interface
- Bridge/Controller



Controller/Bridge HDD v.s. Flash

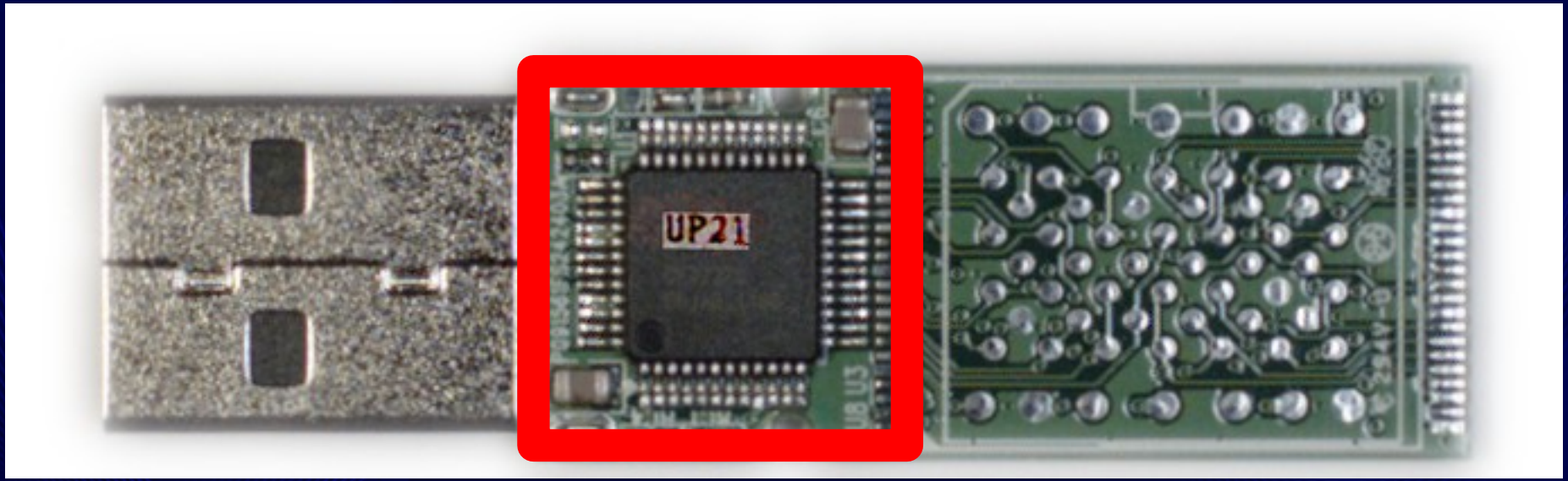
- HDD (Bridge)
  - USB → HDD protocol translation
  - Generic firmware – host sees what is connected
- Flash (Controller)
  - Logical mapping LBAs to Flash Memory
  - Controller can be reprogrammed!
  - Host sees what the controller wants!!


KUMCUAT WALRUS
MIGRAIN FULL BELLY FOCUS
More funny pictures at funnypicsplus.com

USB Flash Drive PCB

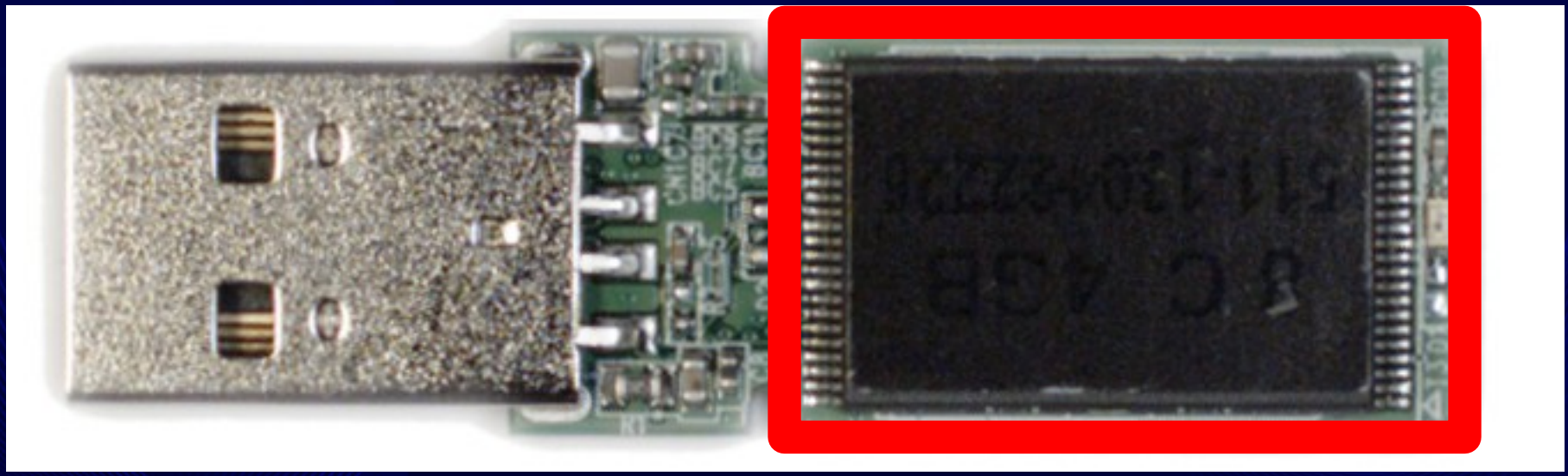
Basic Components of Flash drives

- Controller ASIC
- Flash Memory



Basic Components of Flash drives

- Controller ASIC
- Flash Memory



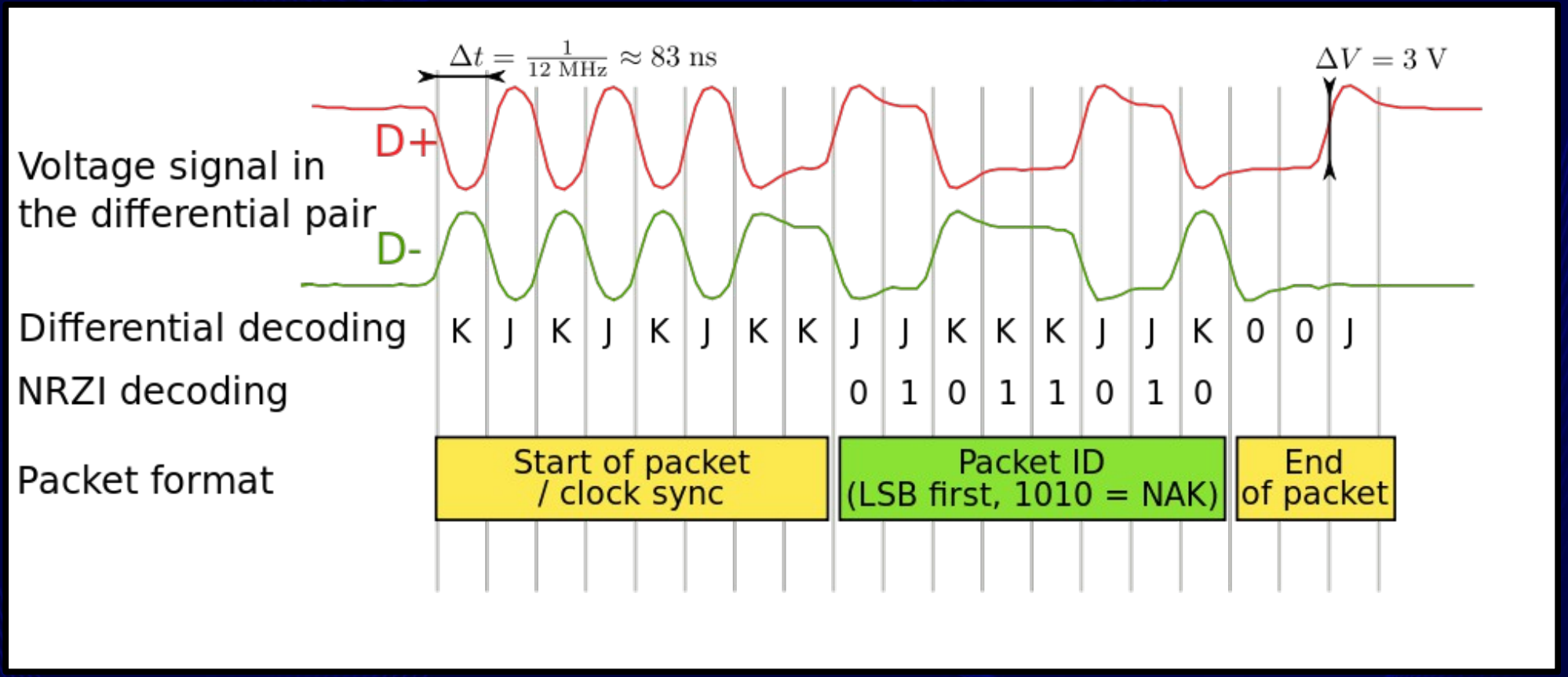
USB Mass Storage

- Signaling: Differential Voltage
- Speed: 6MHz, 12MHz, 24MHz, 2.5GHz (SS)
- Bridge/Controller chip translates USB to storage device
- No direct translation from USB-MS protocol to SATA/IDE protocol or Flash Chips

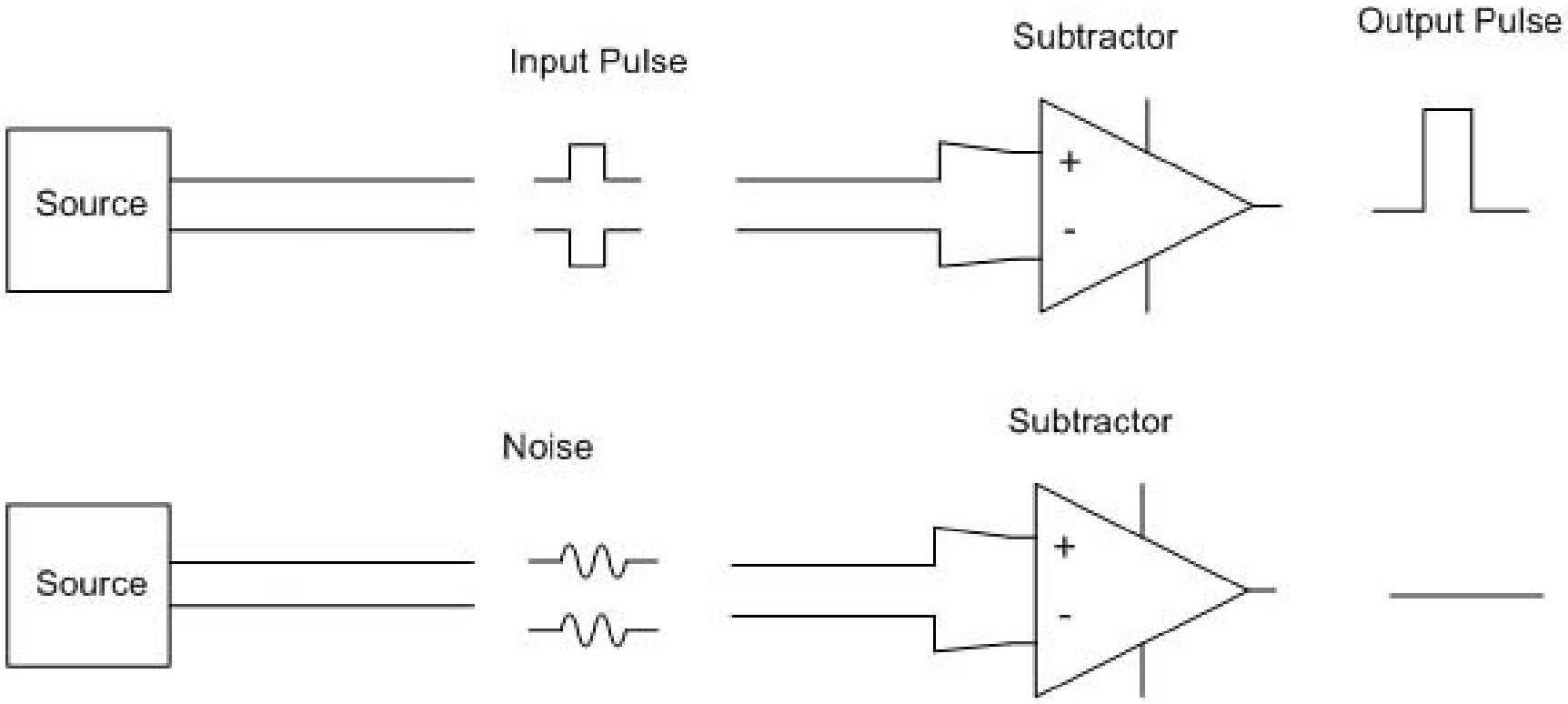
USB Mass Storage == SCSI

- USB-MS is encapsulated SCSI
- Subset of SCSI commands, based on peripheral type
- Encapsulation can cause trouble (smartmon, smartctl, etc)
- Generally one SCSI target, one or more Logical Units (LUNs)

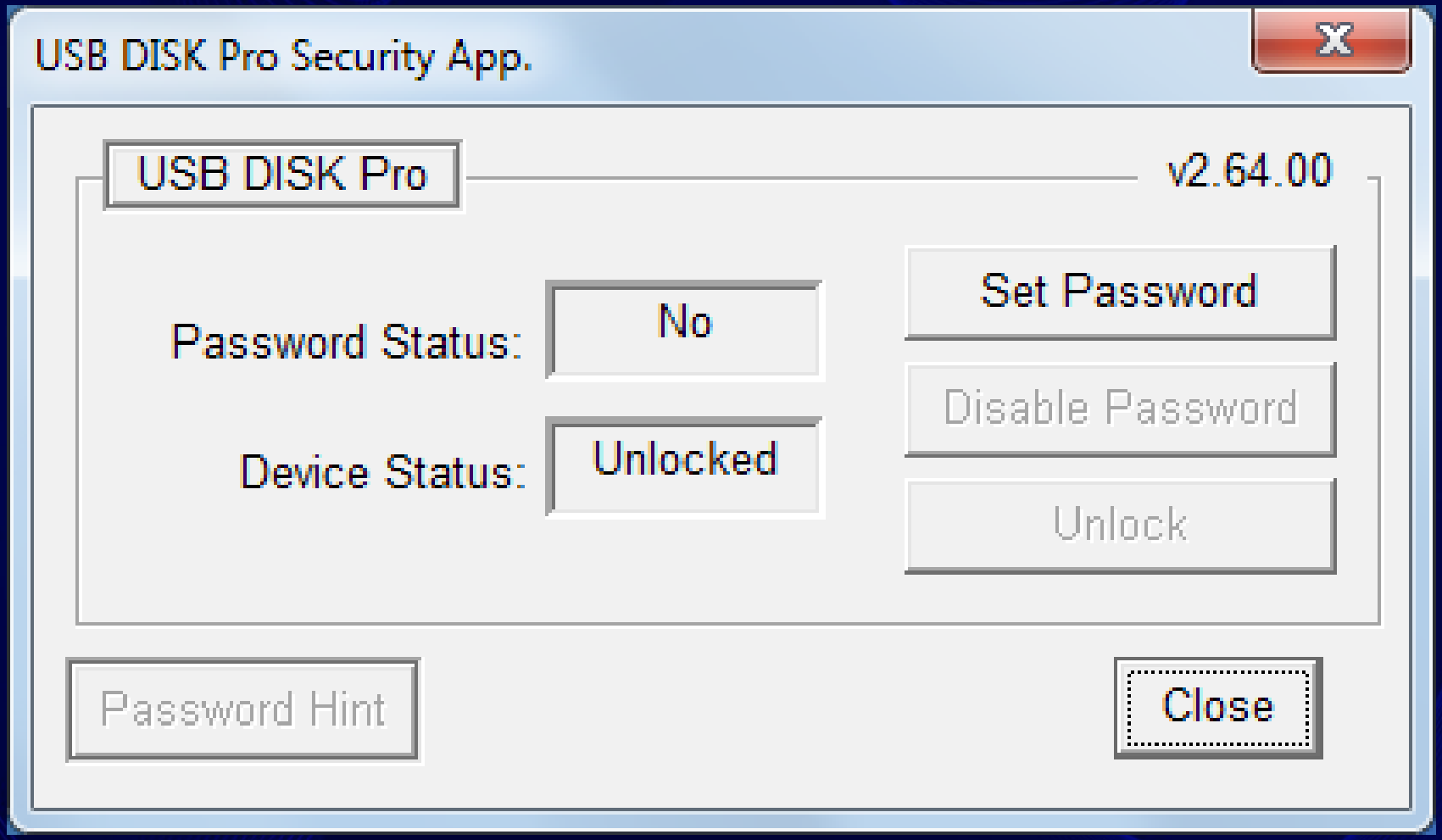
USB signaling



Differential Signaling



Phison Security Tool



Low-Level Sniffing USB

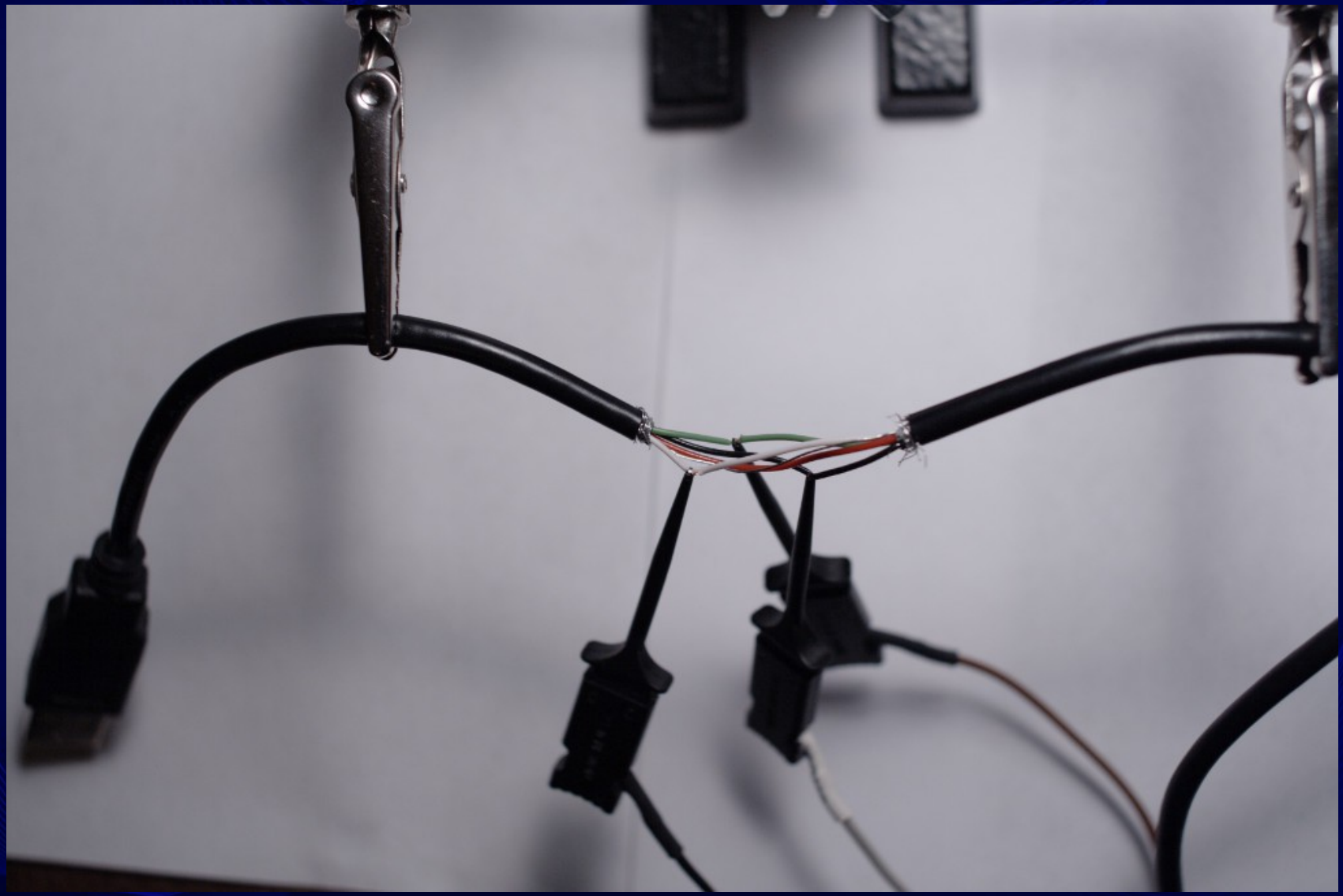
- Logic Analyzer
  - Low level
  - Too much detail
  - No protocol-in-protocol decoding
- Hardware MITM device
  - Low level
  - See Dominic's talk tomorrow

Saleae Logic8

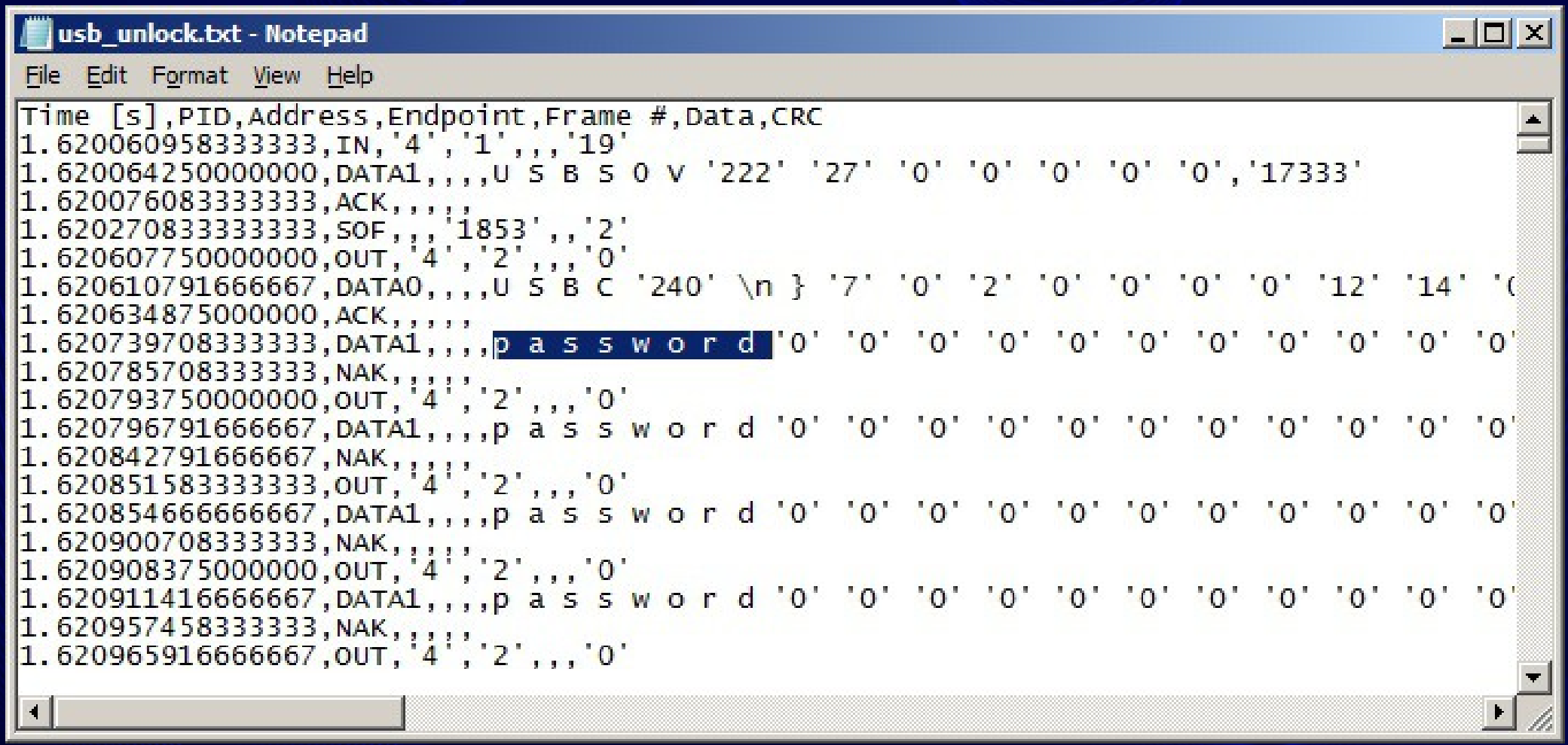
- USB2 based logic analyzer
- v1.1.18 beta software supports USB
- USB2 sniffing a USB2 device? Inconceivable!
  - Use a USB1 hub to slow down target.
  - Vampire tap lines

Sniffing rig
(USB extension cable)

Sniffing rig



Results! ... no context though

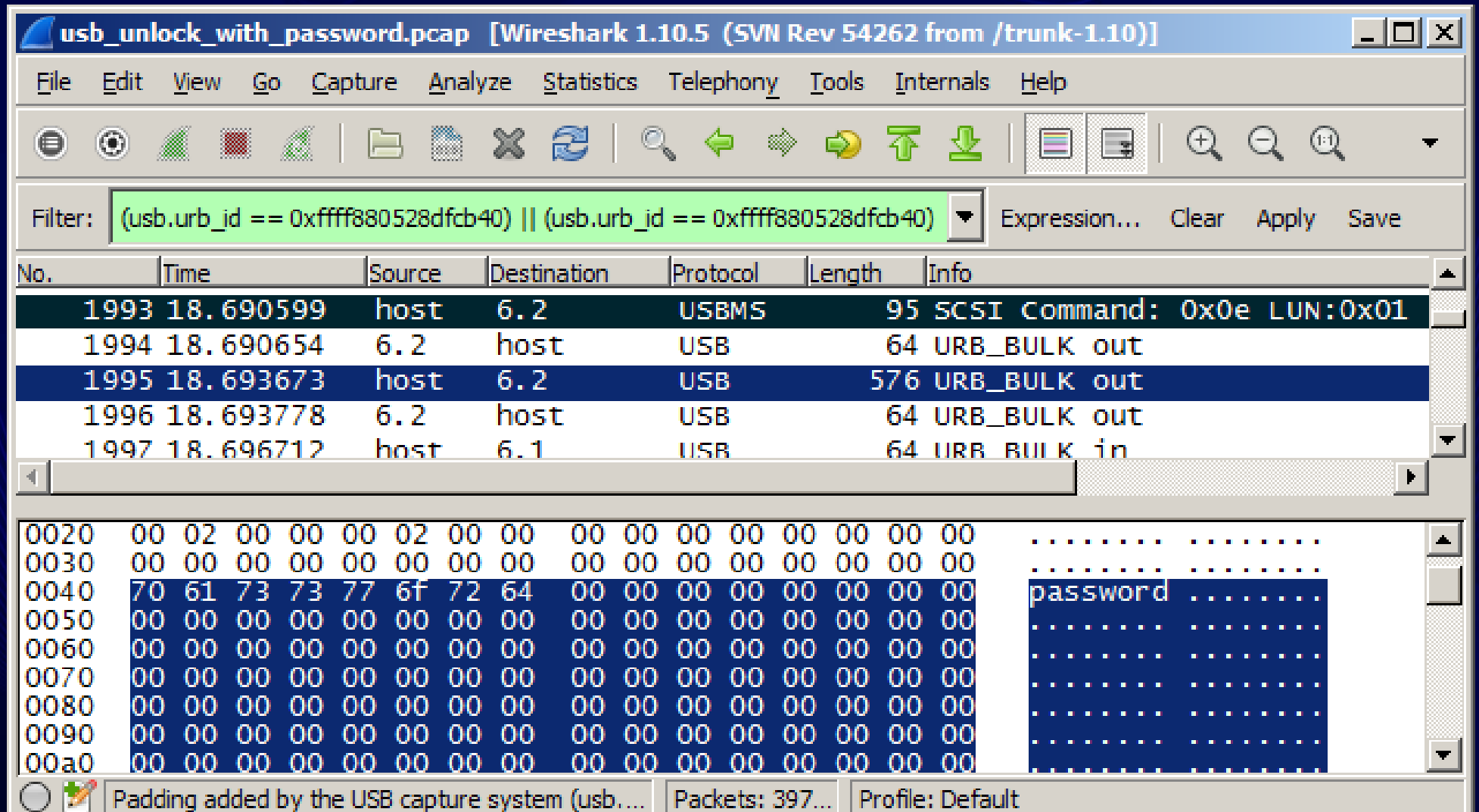


High-Level Sniffing USB

- USBPcap (self-snoop) + Wireshark
  - Windows, High level, can/will miss data
- Virtualization dumping USB
  - Full & complete dump
- Linux usbmon → tcpdump -i usbmon2
  - Lots of tools to inspect
  - Wireshark!
    - USB decoding, USB-MS decoding

Sniffing USB

Virtualization + usbmon dumping USB



Re-implementing USB Flash Drive Security Features Under Linux

- Disable LUN Protection:

```
# echo -n password | sg_raw -s 8 /dev/sg3 \
0E 00 01 55 AA 00
```

- Unlock LUN:

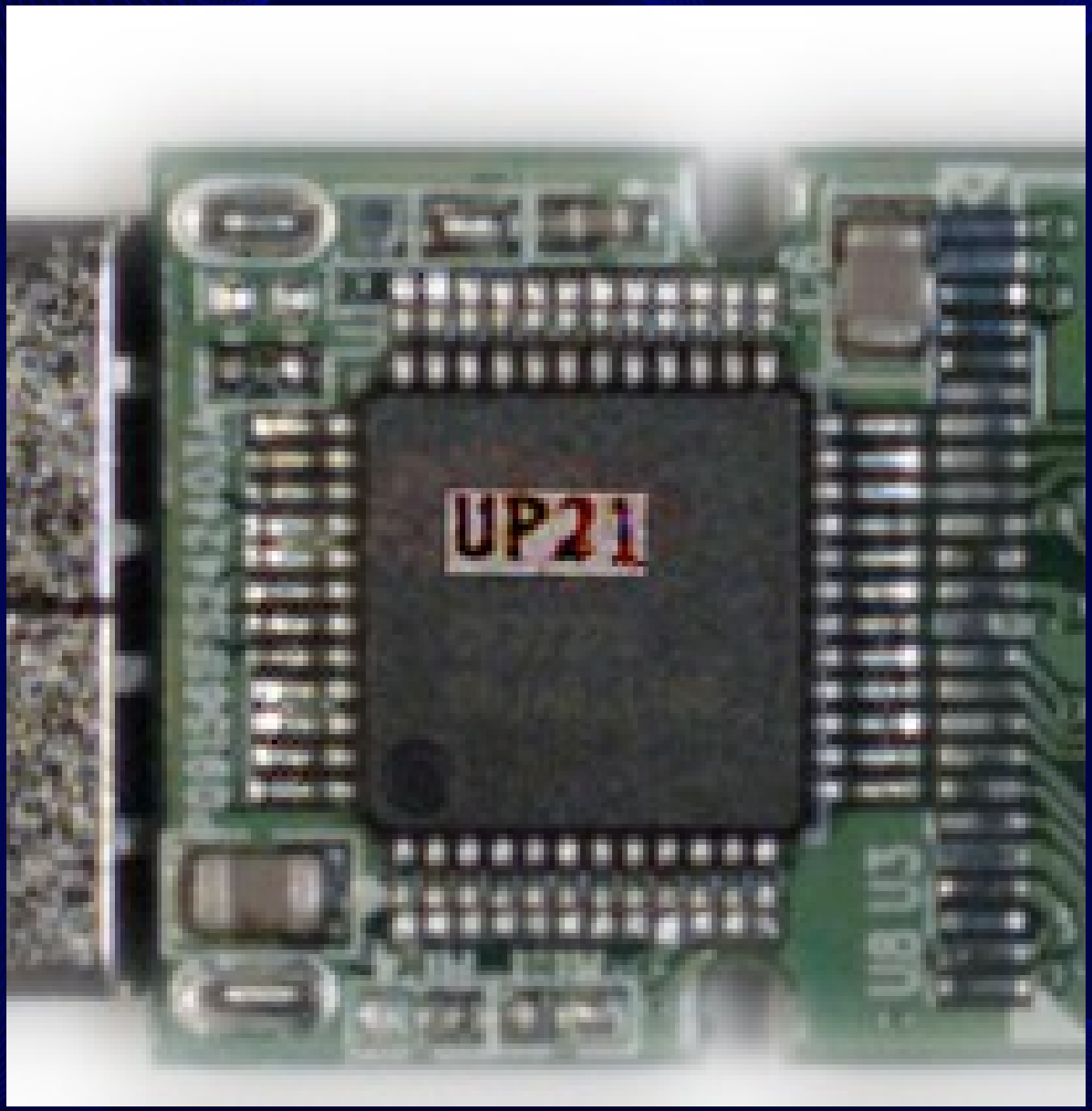
```
# echo -n password | sg_raw -s 8 /dev/sg3 \
0E 00 00 00 00 00
```

Re-implementing USB Flash Drive Security Features Under Linux

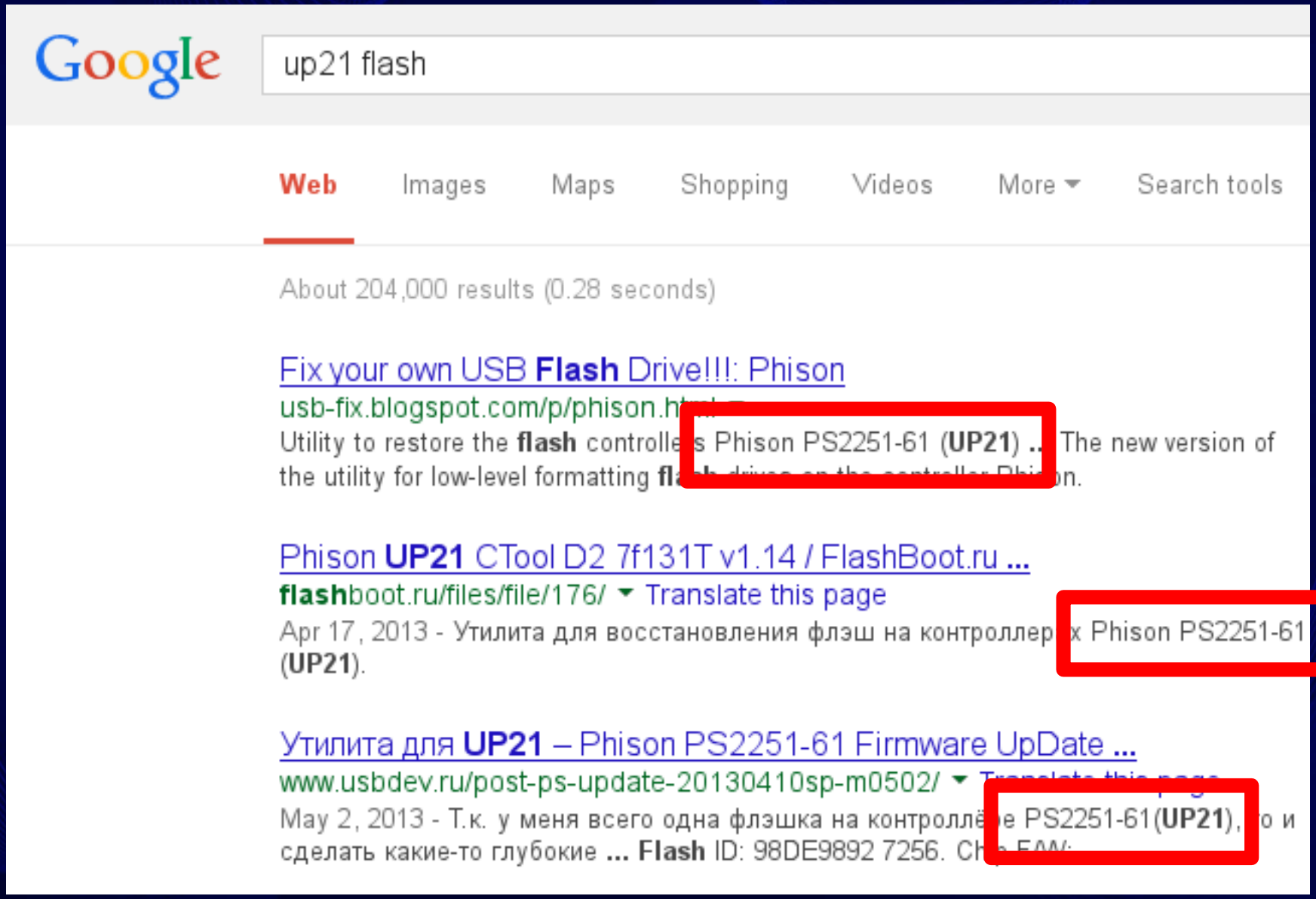
- Change Password / Lock LUN:

```
# perl -e 'print pack("a16 a16 a32",
  "old pass", "new pass", "pw hint")' | \
sg_raw -v -s 64 /dev/sg3 0E 06 01 00 00 00
```

UP21 Flash Controller



UP21 Flash Controller



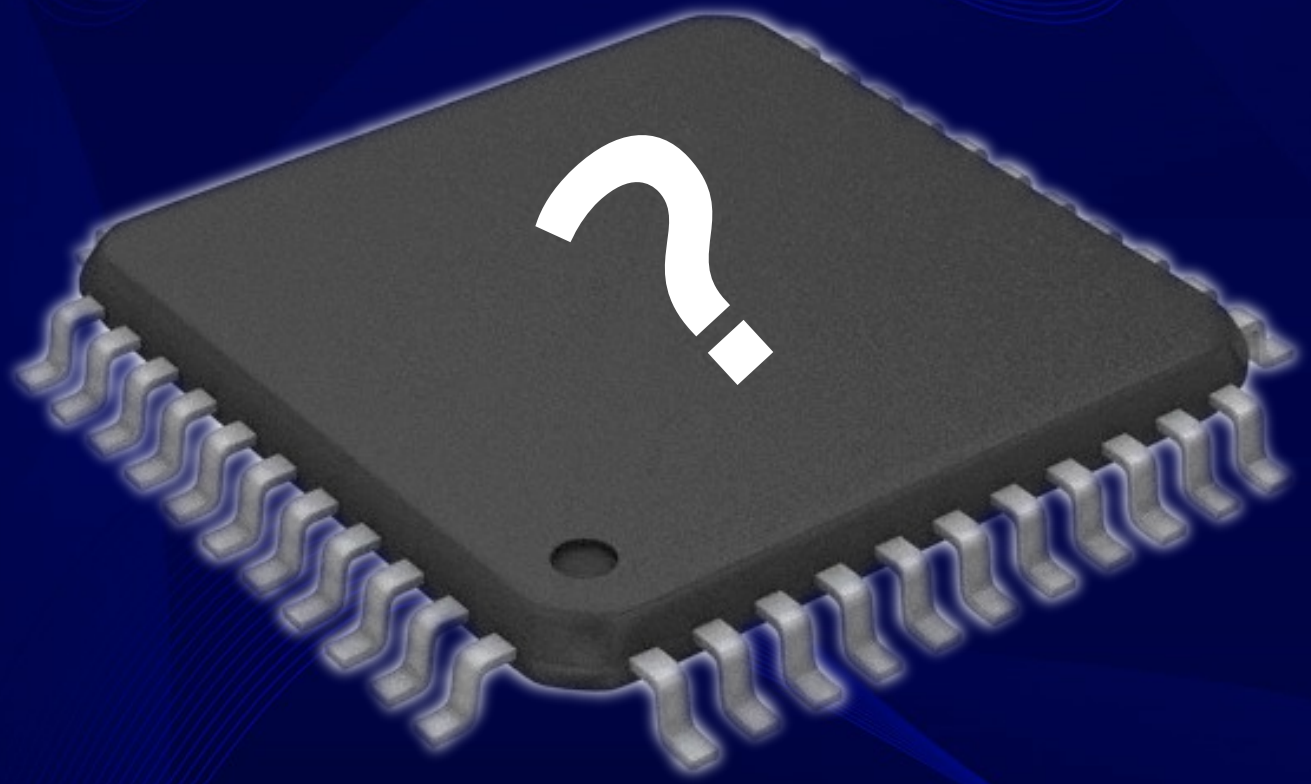
Consumer Flash *Drive* Vendors

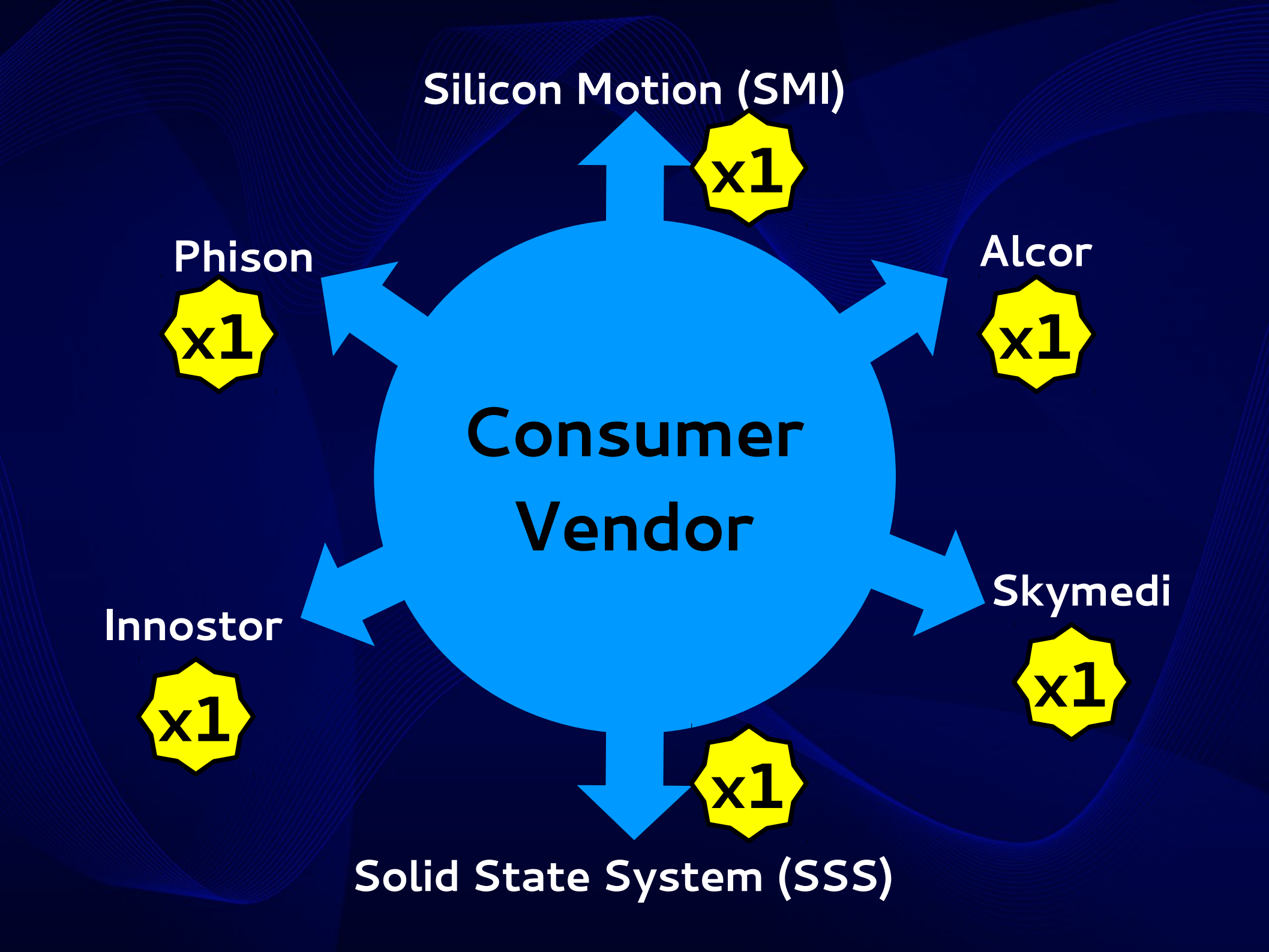
- SanDisk
- Kingston Digital
- Lexar
- PNY
- HP
- Sony
- TDK
- Patriot
- ADATA
- Silicon Power
- Transcend
- Verbatim
- Toshiba
- Lenovo

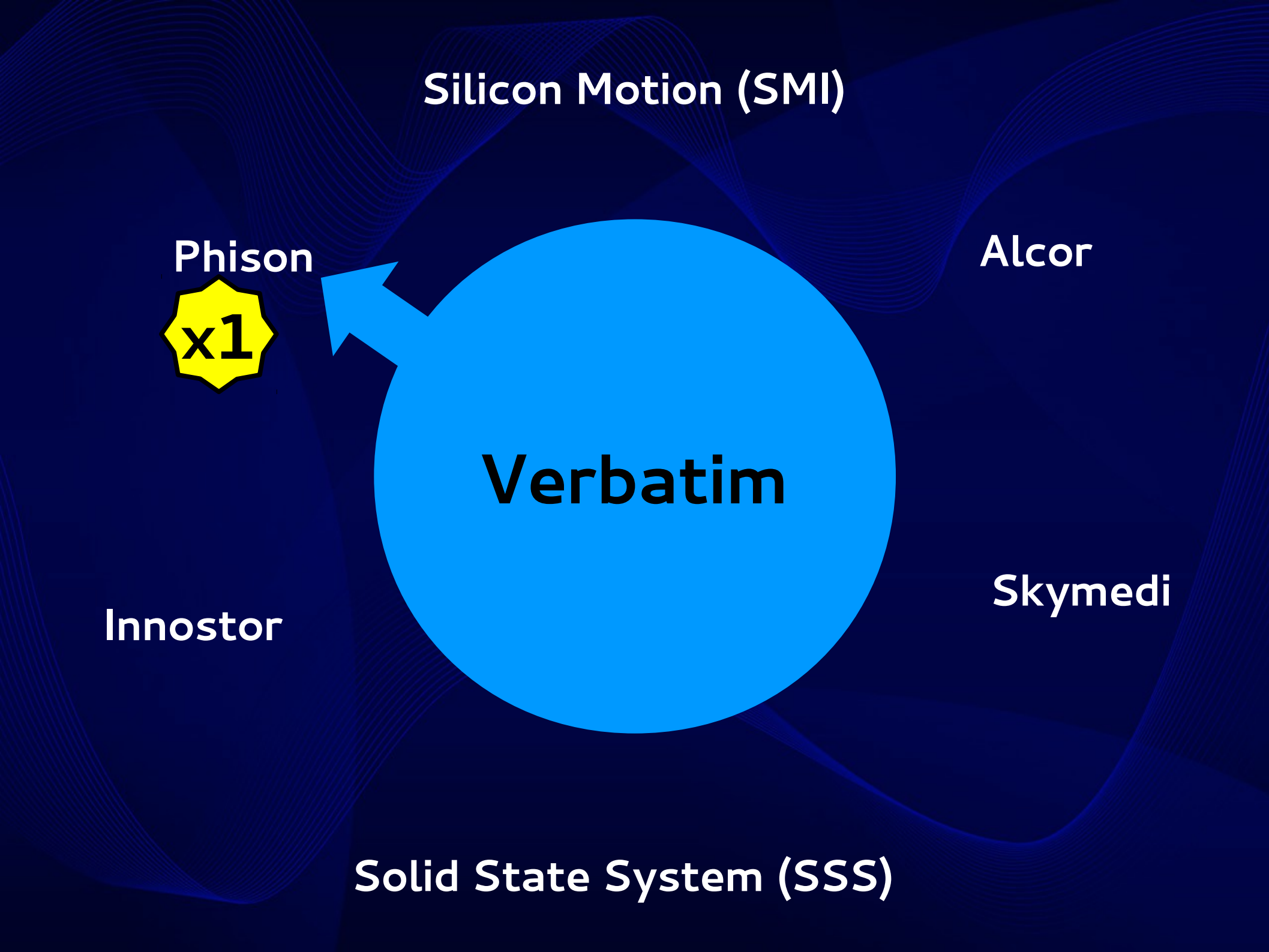
OEM Flash *Controller* Vendors

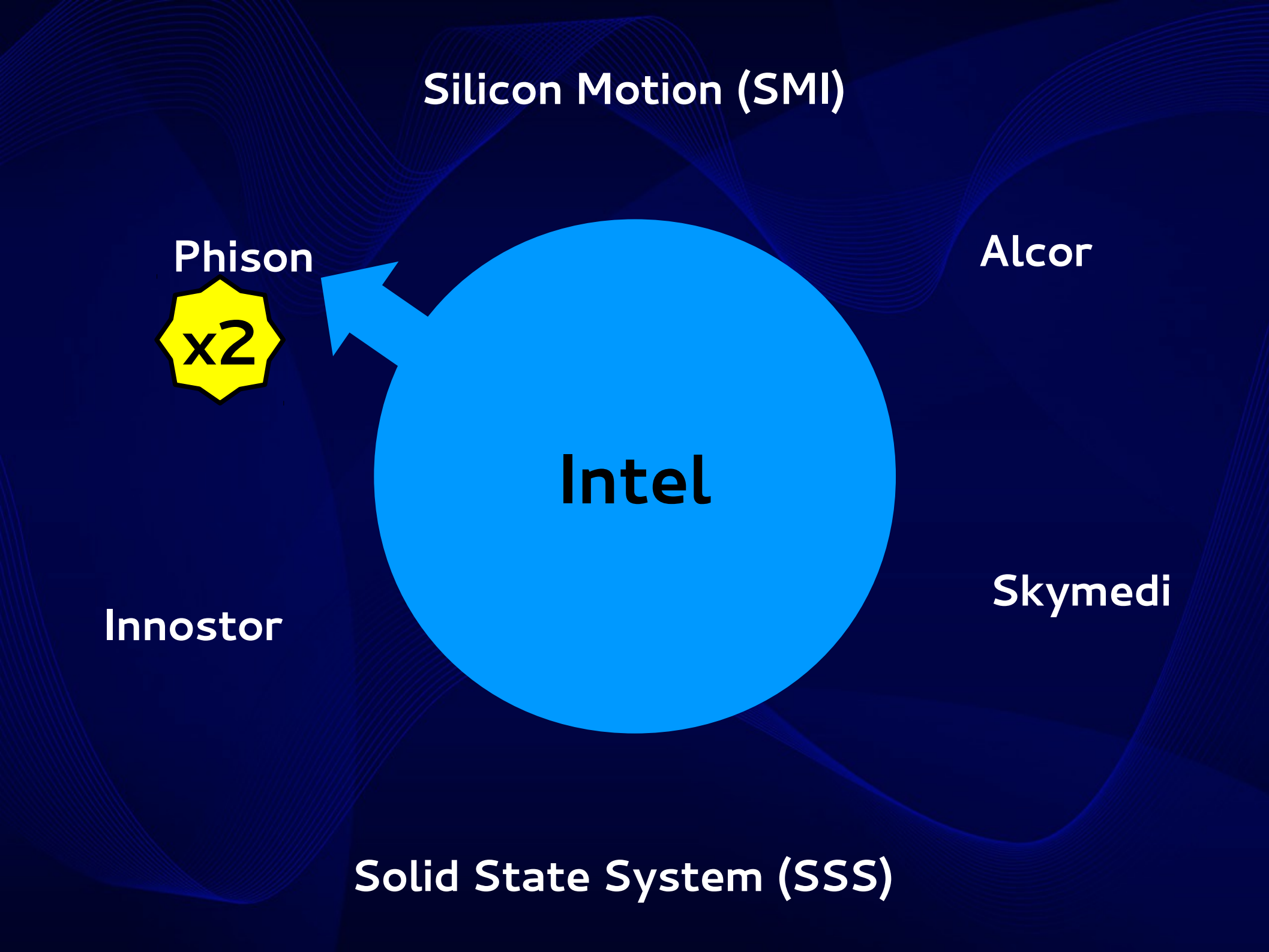
- Phison
- ALCOR
- Innostor
- Skymedi
- Silicon Micro
- Solid State System
- USBest
- Ameco
- ChipsBank
- Efortune
- Icreate
- Netac
- OTI
- Prolific

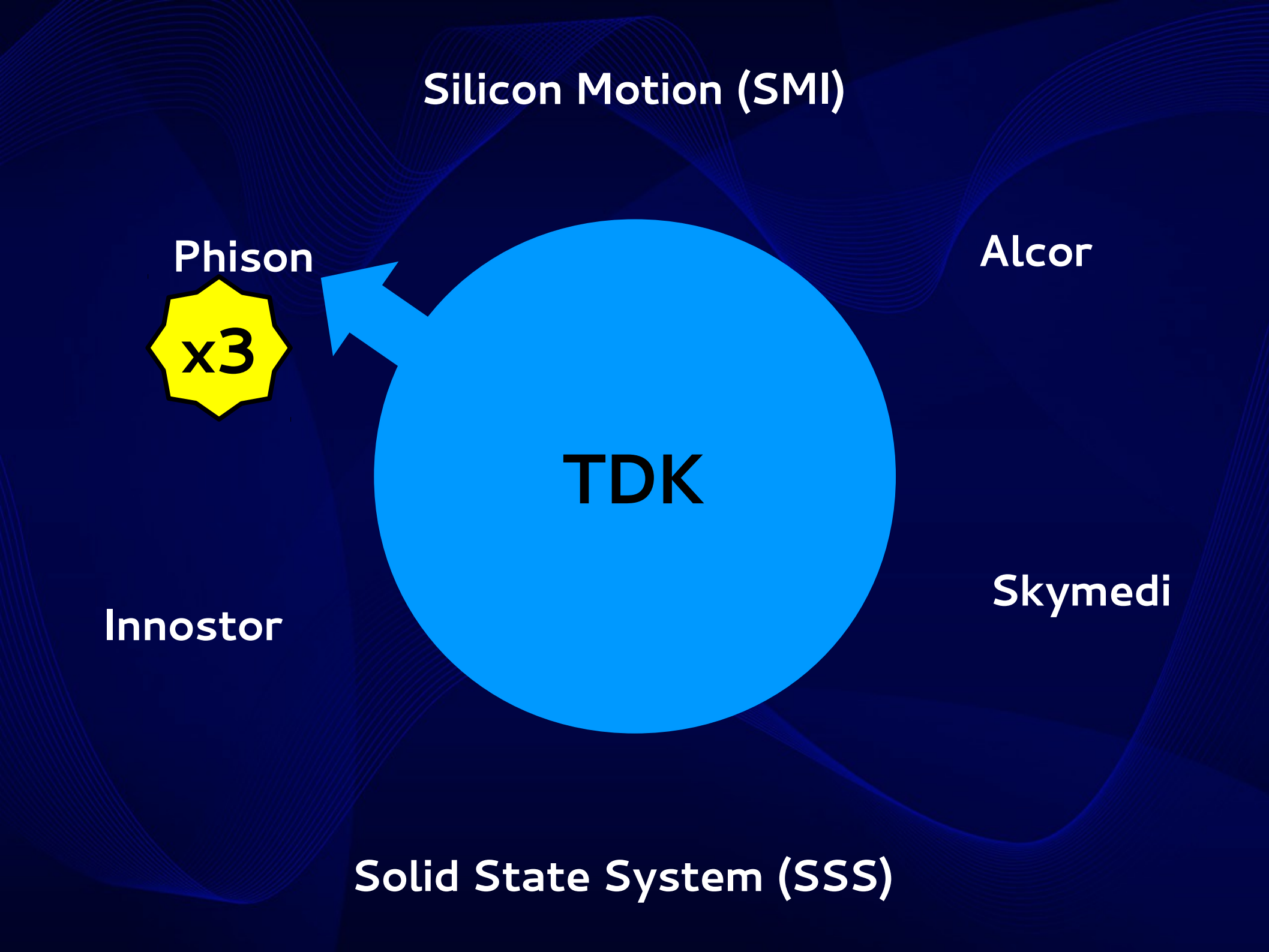
Who uses what?

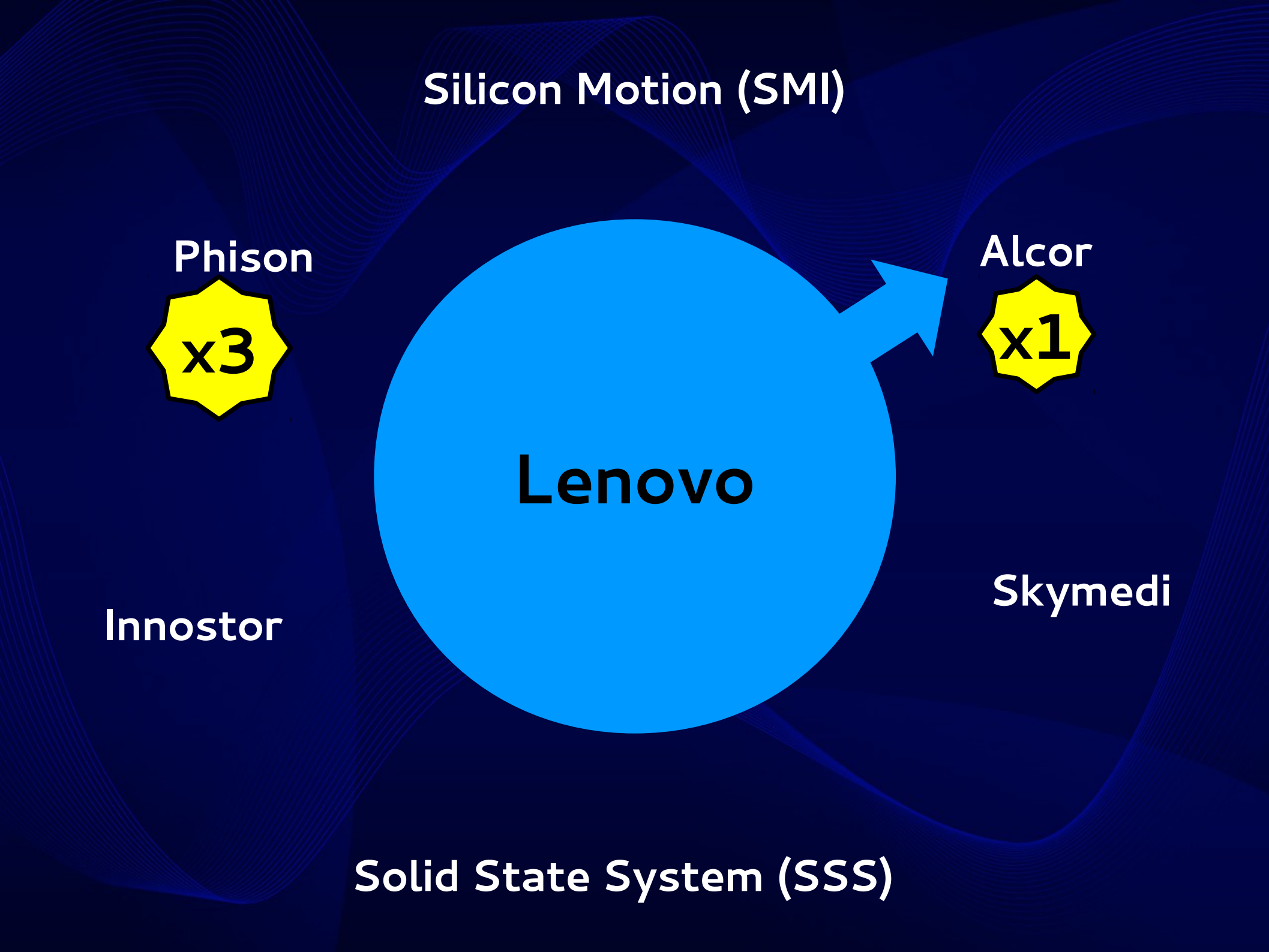


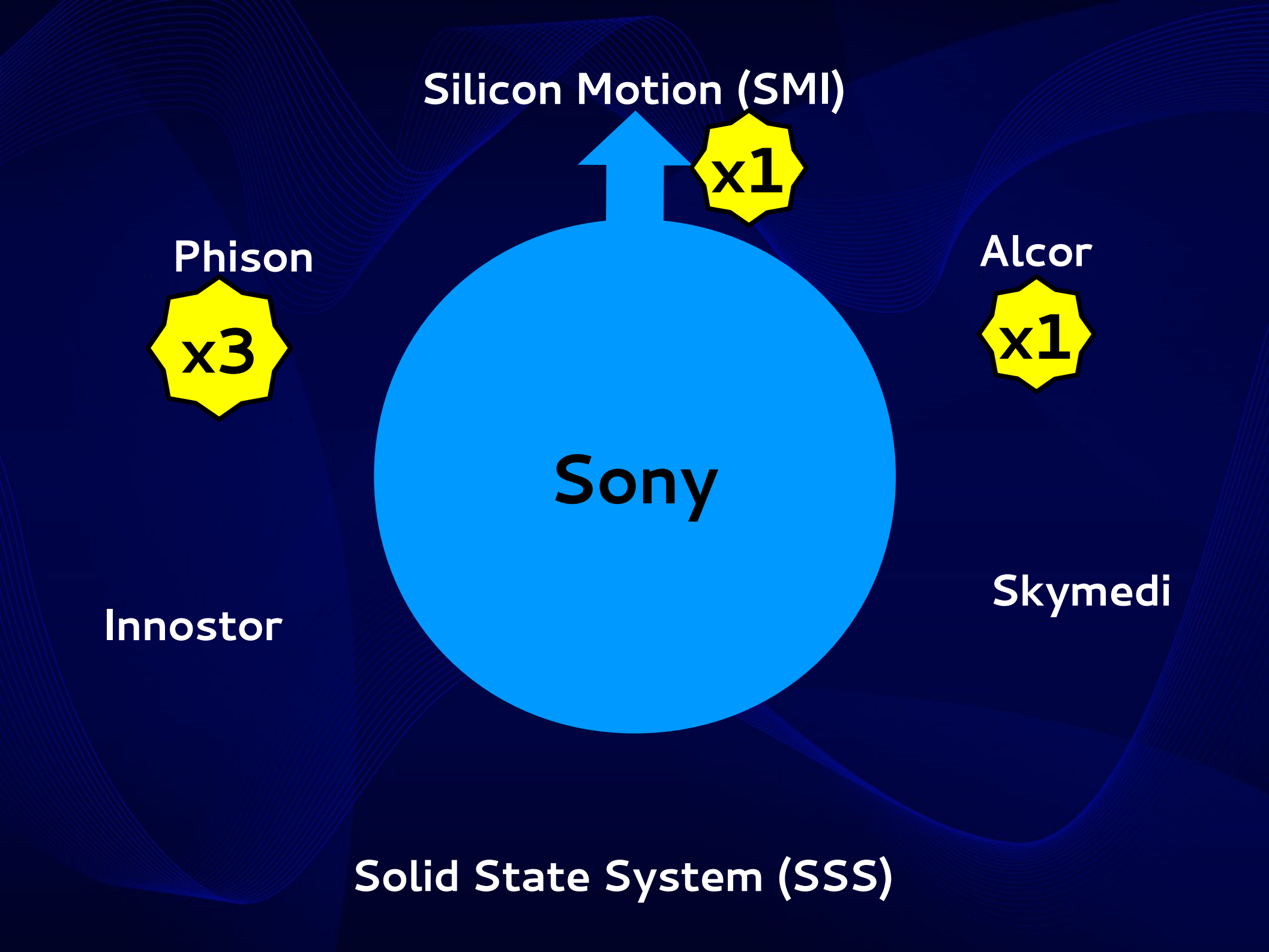

Silicon Motion (SMI)
x1
Phison
x1
Alcor
x1
Consumer
Vendor
Innostor
x1
Skymedi
x1
x1
Solid State System (SSS)

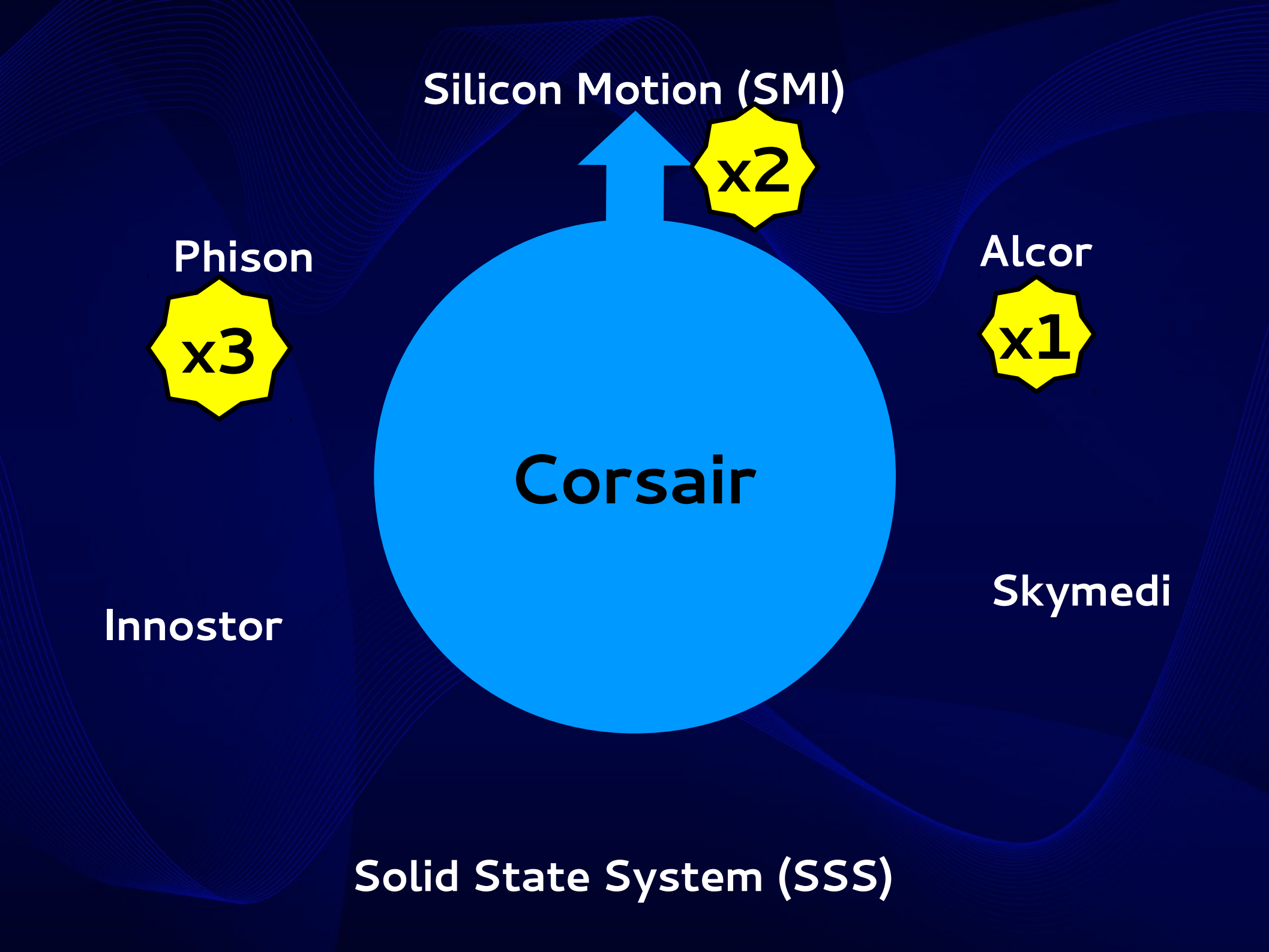

Silicon Motion (SMI)
Phison
x1
Alcor
Verbatim
Innostor
Skymedi
Solid State System (SSS)

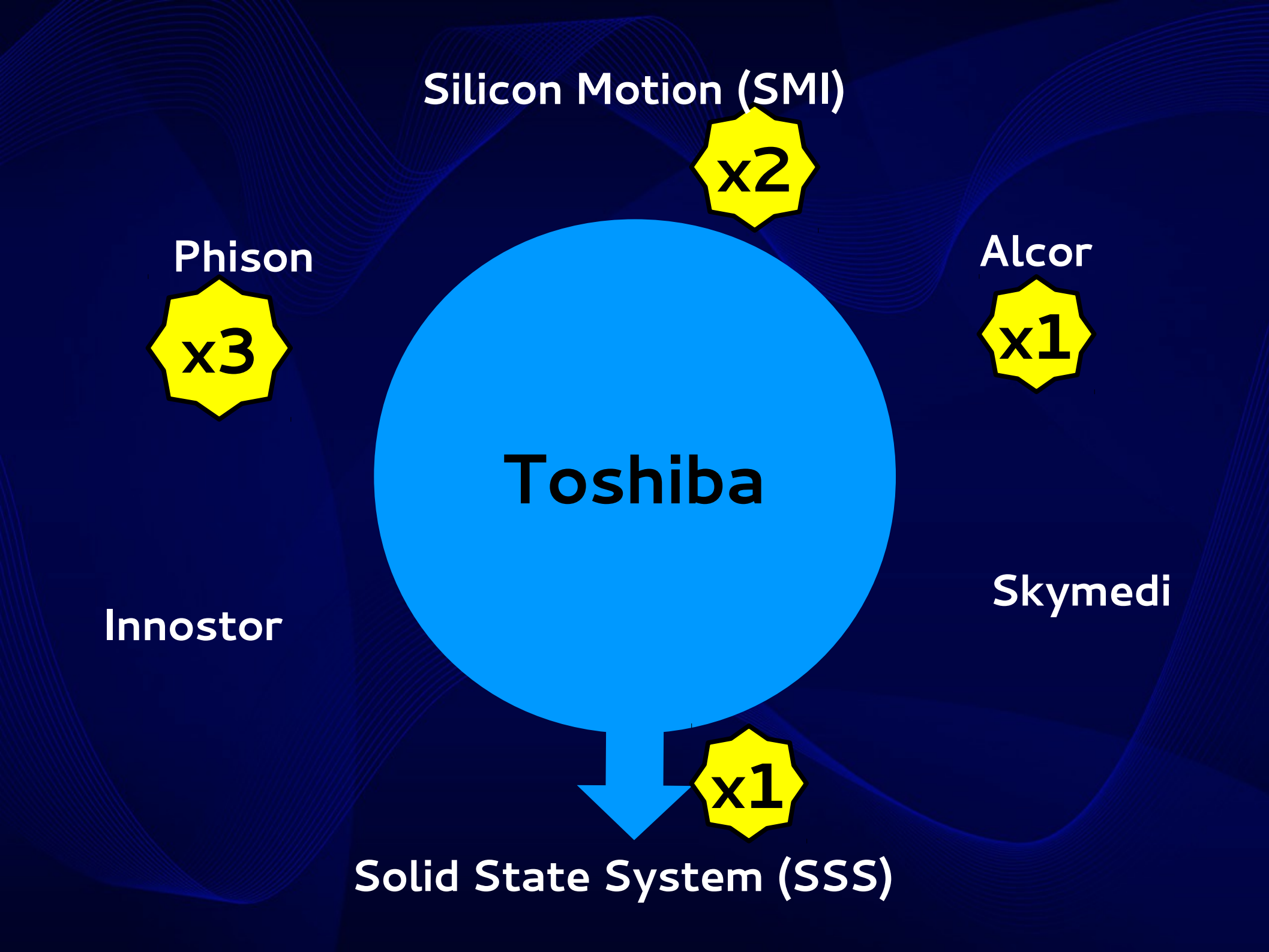

Silicon Motion (SMI)
Phison
x2
Alcor
Intel
Skymedi
Innostor
Solid State System (SSS)

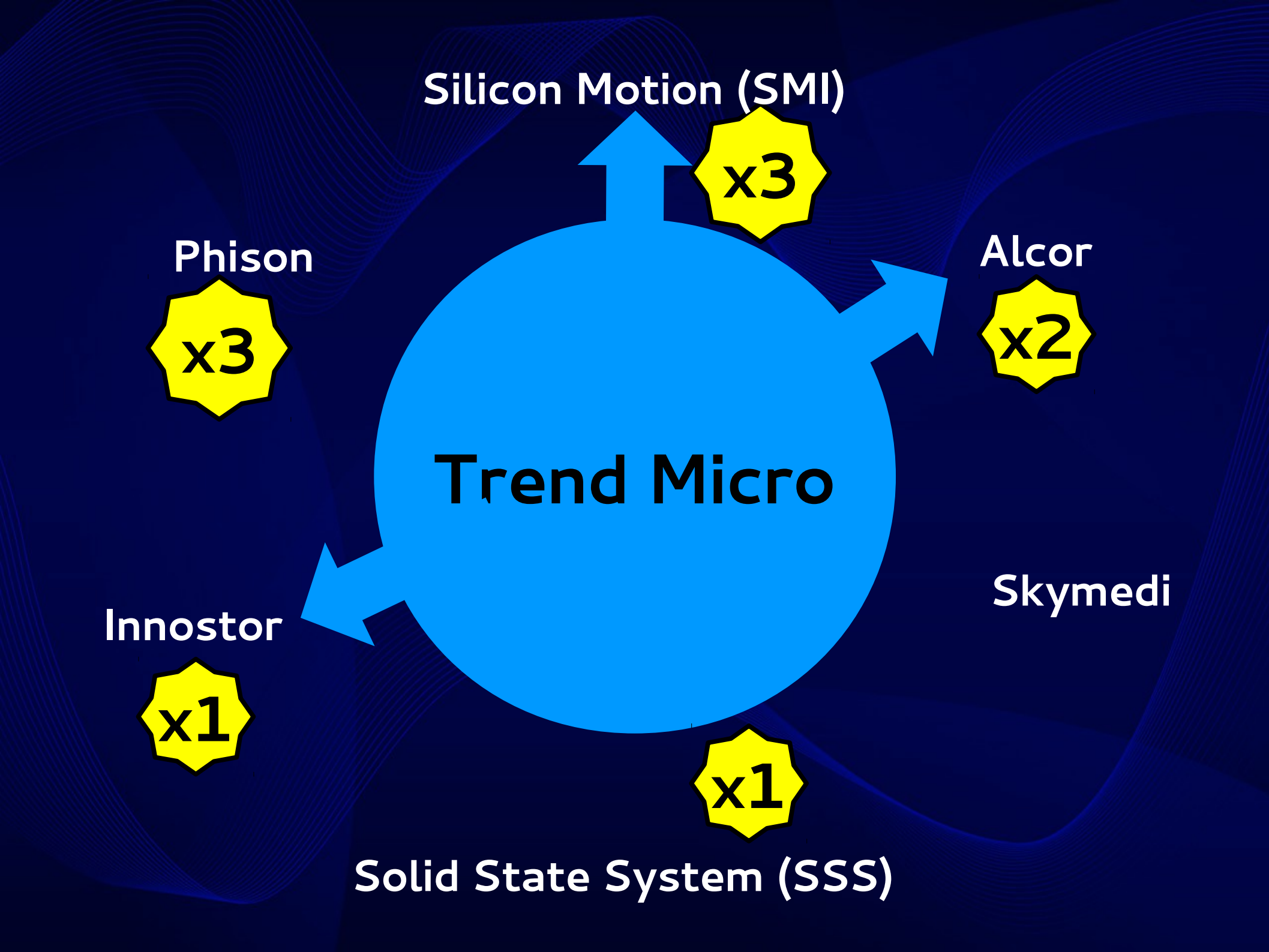

Silicon Motion (SMI)
Phison
x3
Alcor
TDK
Innostor
Skymedi
Solid State System (SSS)

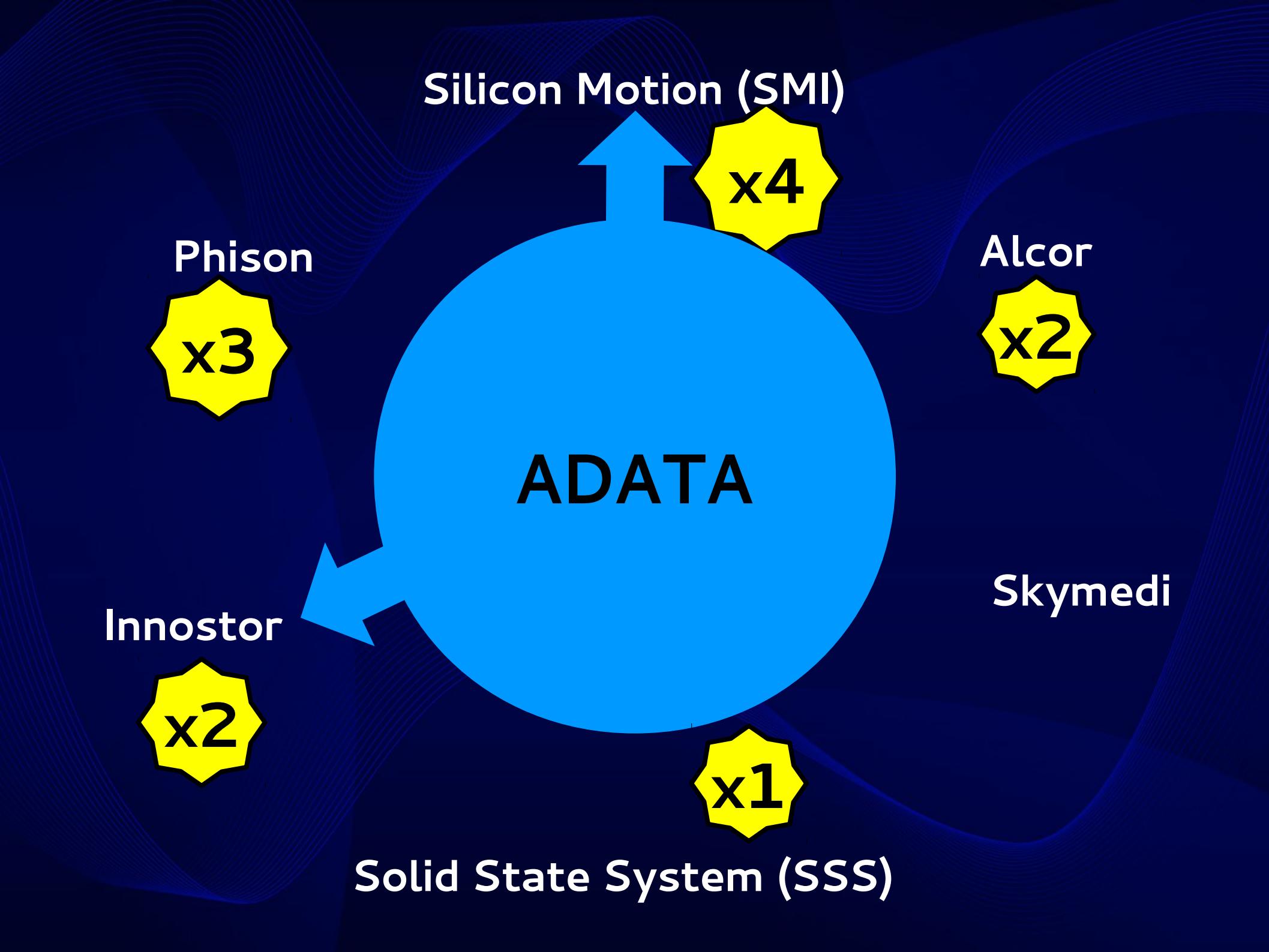

Silicon Motion (SMI)
Phison
x3
Alcor
x1
Lenovo
Skymedi
Innostor
Solid State System (SSS)

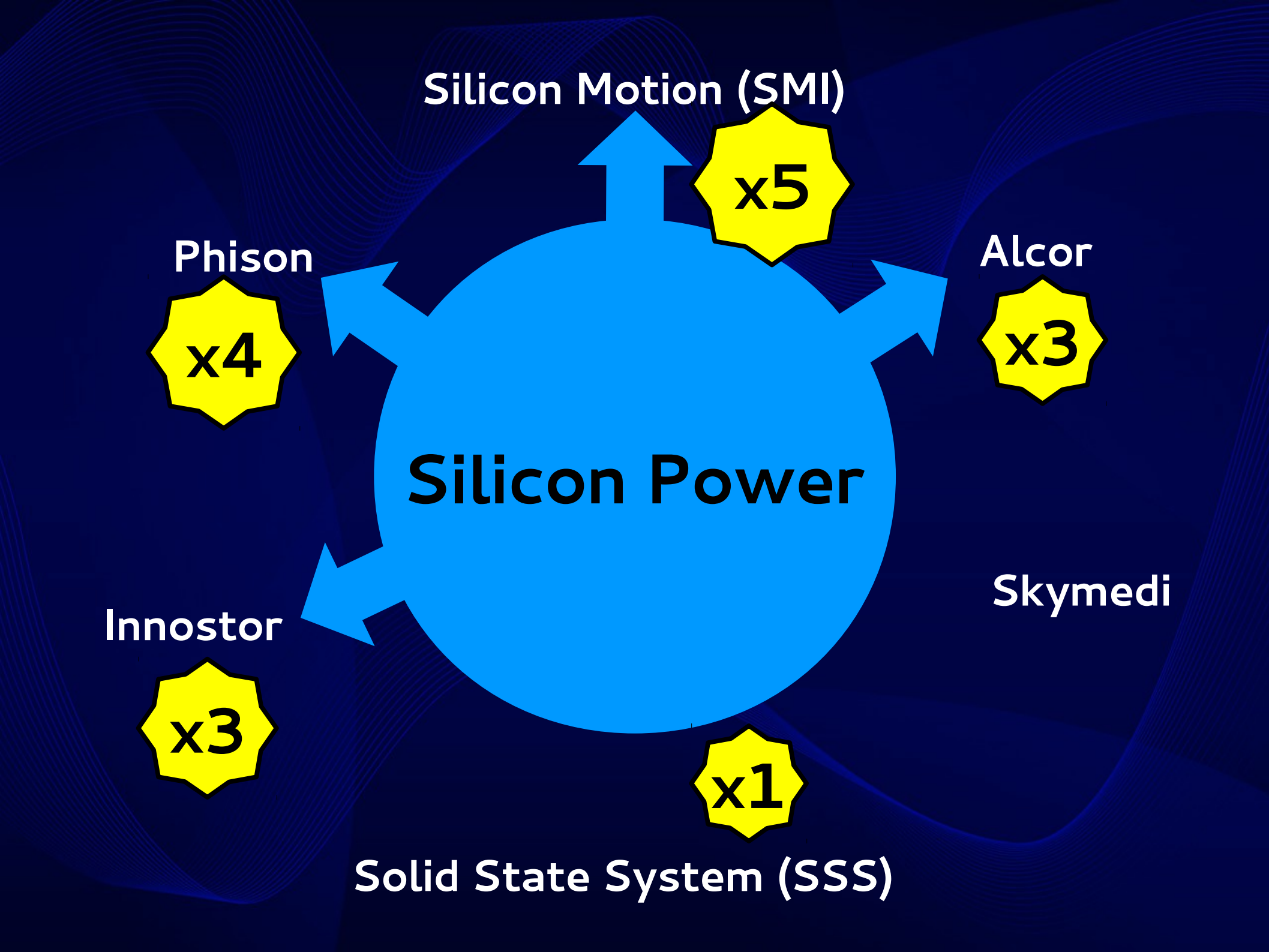

Silicon Motion (SMI)
x1
Phison
x3
Alcor
x1
Sony
Innostor
Skymedi
Solid State System (SSS)

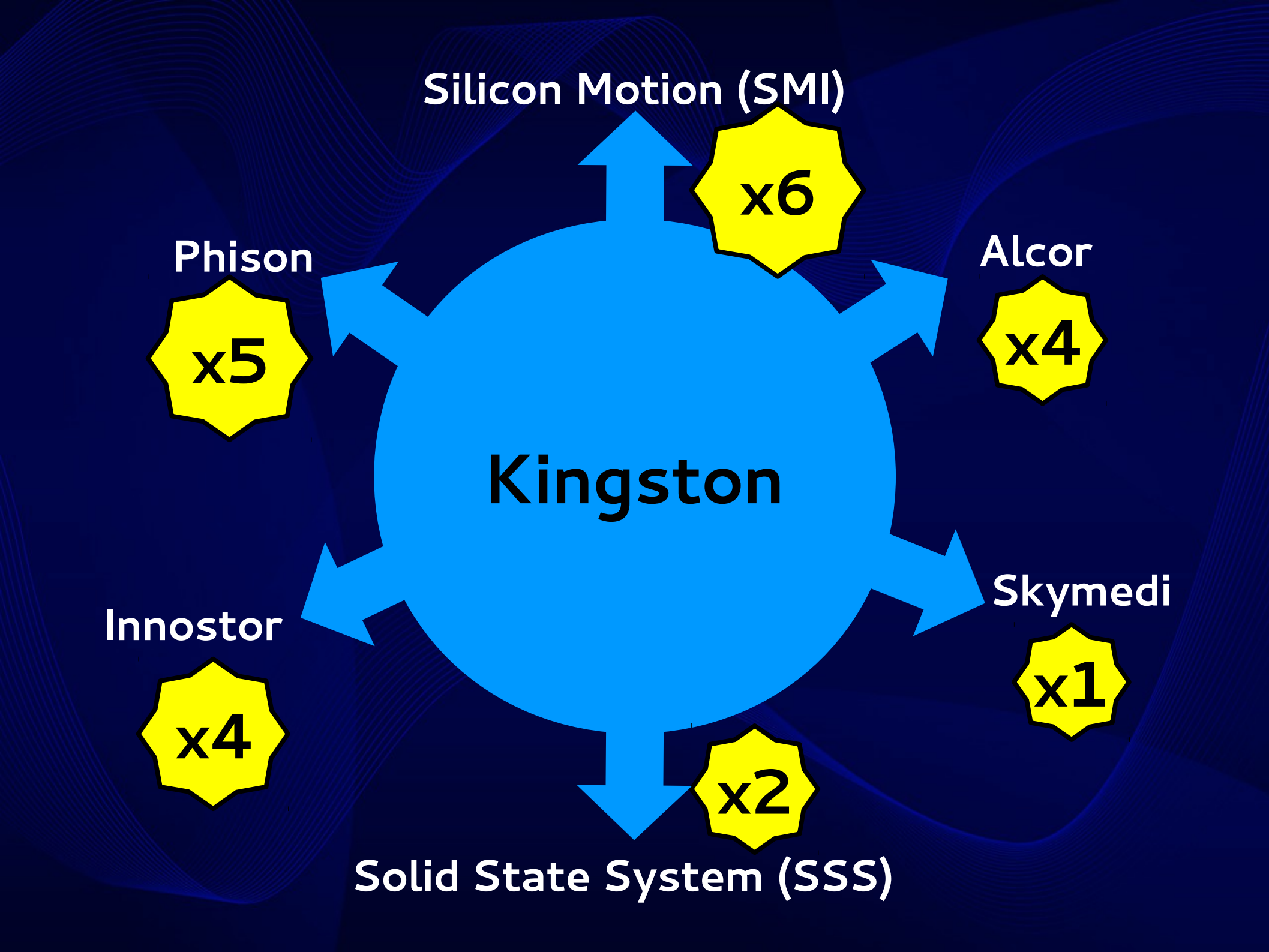

Silicon Motion (SMI)
x2
Phison
x3
Alcor
x1
Corsair
Innostor
Skymedi
Solid State System (SSS)


Silicon Motion (SMI)
x2
Phison
x3
Alcor
x1
Toshiba
Skymedi
Innostor
x1
Solid State System (SSS)


Silicon Motion (SMI)
x3
Phison
x3
Alcor
x2
Trend Micro
Innostor
x1
Skymedi
x1
Solid State System (SSS)


Silicon Motion (SMI)
x4
Phison
x3
Alcor
x2
ADATA
Innostor
x2
Skymedi
x1
Solid State System (SSS)

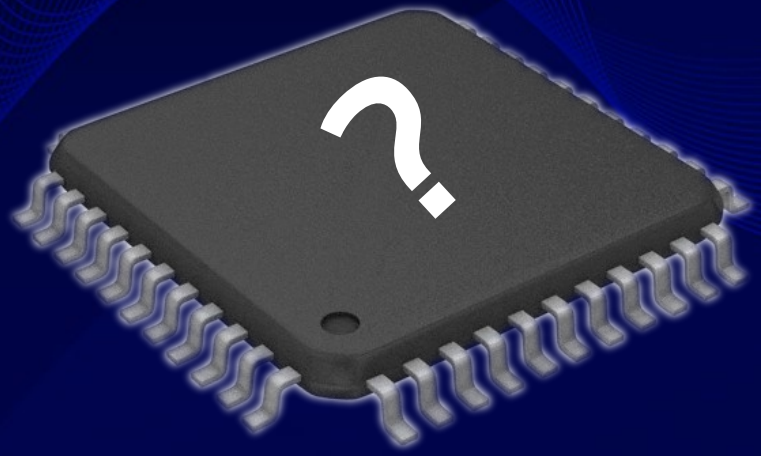

Silicon Motion (SMI)
x5
Phison
x4
Alcor
x3
Silicon Power
Skymedi
Innostor
x3
x1
Solid State System (SSS)


Silicon Motion (SMI)
x6
Phison
x5
Alcor
x4
Kingston
Innostor
x4
Skymedi
x1
x2
Solid State System (SSS)

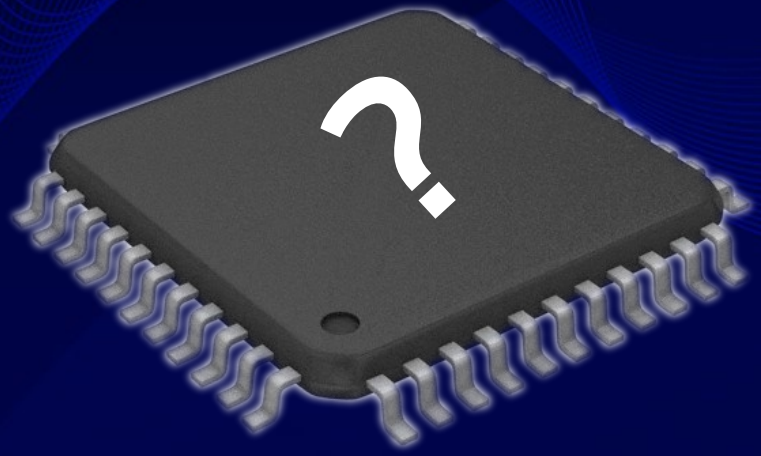
Flash drive lineup

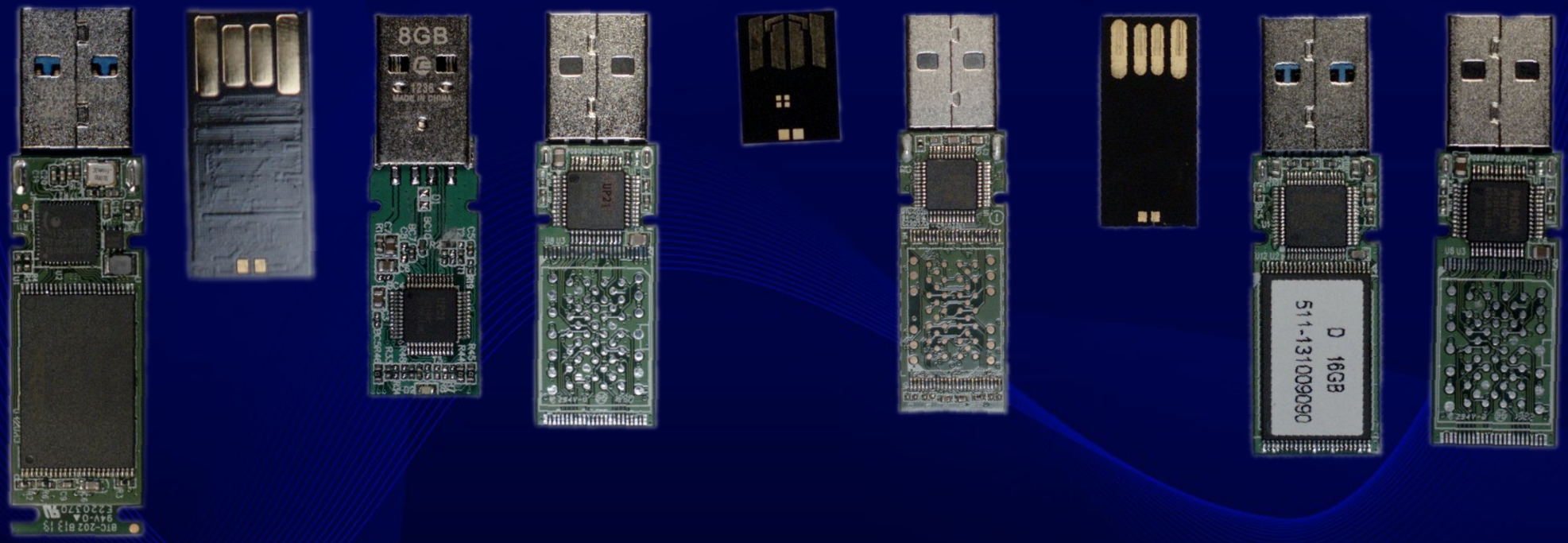
- All purchased at Micro Center
- Tried to get as different as possible .....

Which controller?

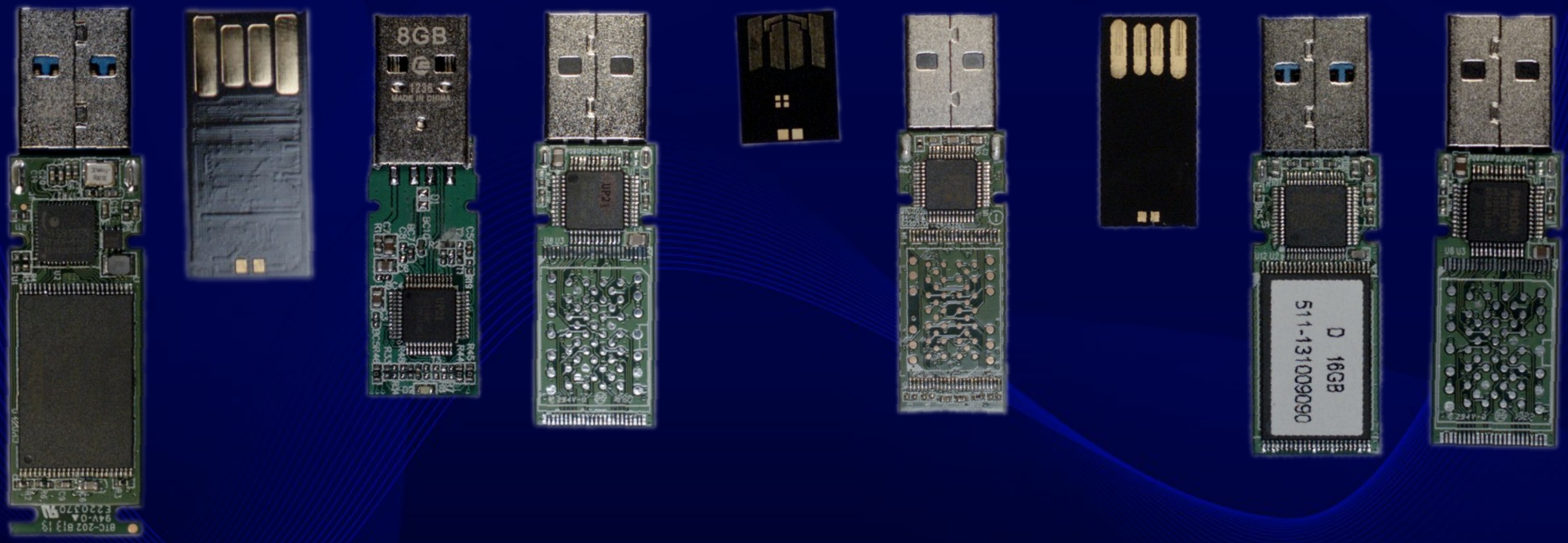


Which controller brand?





Which controller brand?

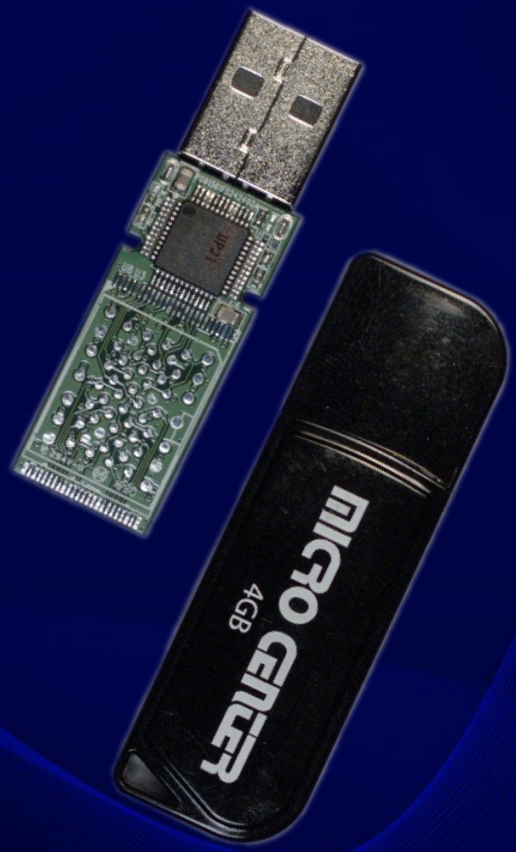


Flash Lineup: Controller Chips

Count	Brand	Chip
1	Innostor	IS916E
2	Phison	PS2251-61
1	Phison	PS2261-68
1	Phison	PS2251-03
1	Phison	PS2251-67
2	Silicon Motion	SM3257ENLT

Microcenter 4G USB2

- 4G @ $5
- Phison PS2251-61
  - Supports multiple LUNs
  - Supports hidden LUNs
  - Supports PW protected LUNs

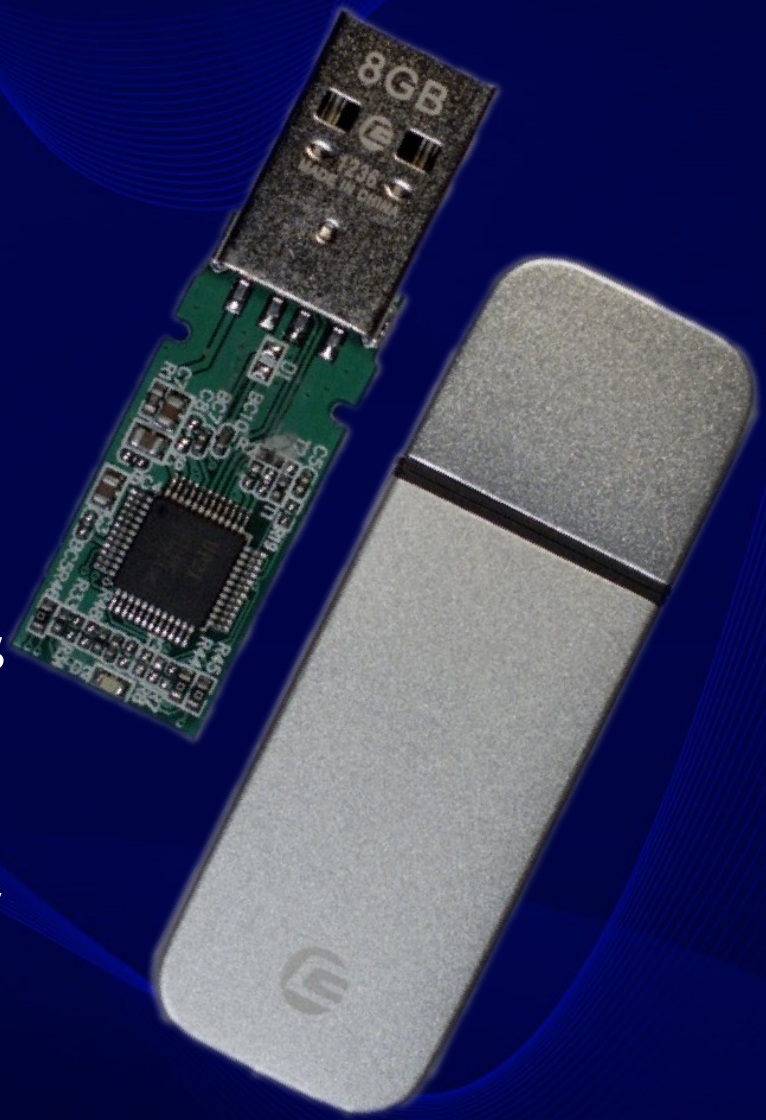


Centeon
Jezebel Licorice

- 8GB @ $8
- SMI SM3257ENLT
  - Supports multiple LUNs
  - Supports hidden LUNs
  - Supports PW protected LUNs

Centeon Secure

- 8GB @ $17
- Phison 2251-61
  - Supports multiple LUNs
  - Supports hidden LUNs
  - Supports PW protected LUNs
- No HW Crypto support
- Contains LUN w/ crypto SW



Which would you buy?

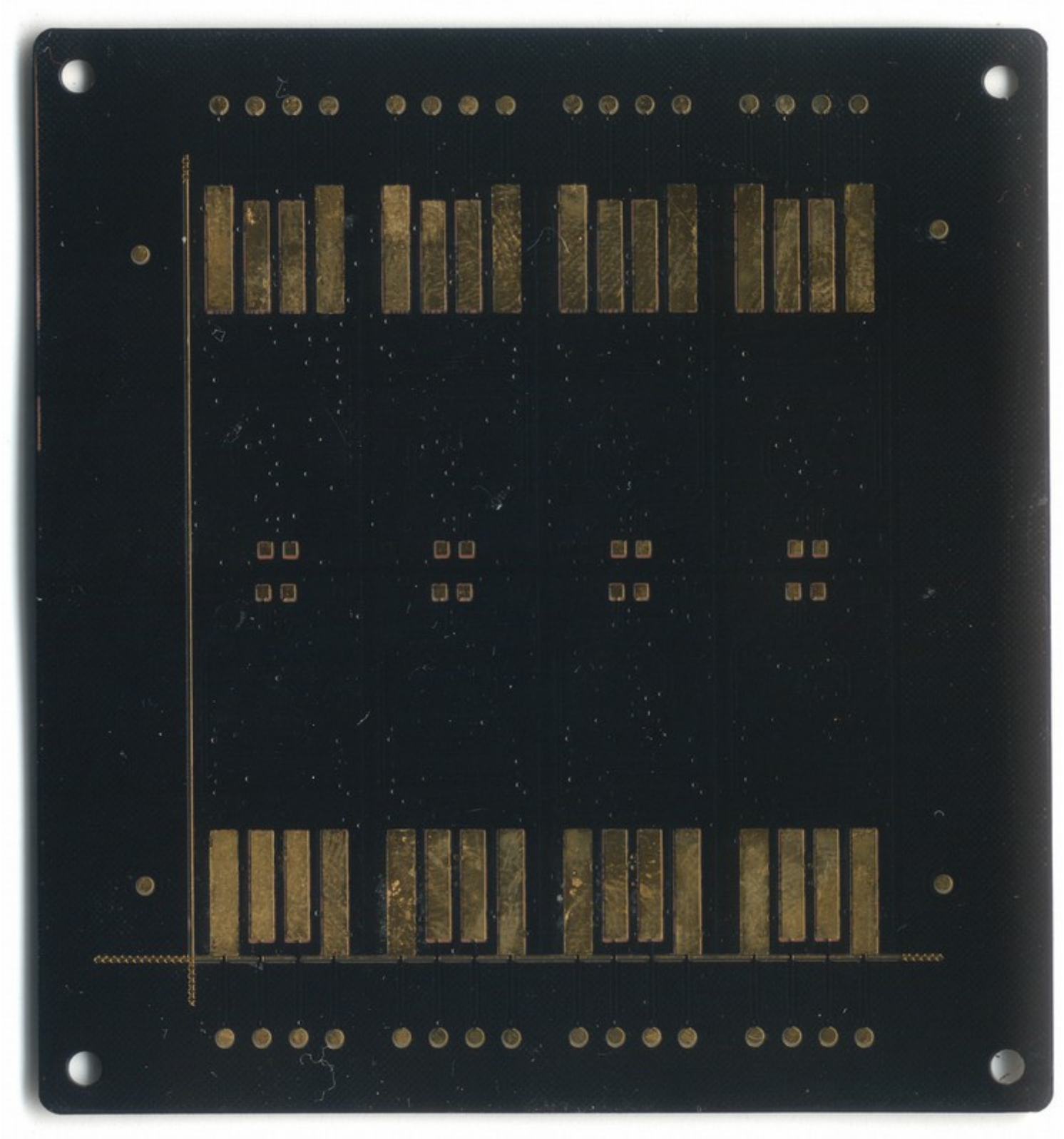
- 8GB @ $8 Centeon Jezebel Licorice
  - All the Flash controller features
  - Use FREE PGP or Truecrypt

OR

- 8GB @ $17 Centeon Secure
  - 2x as expensive
  - No additional benefits

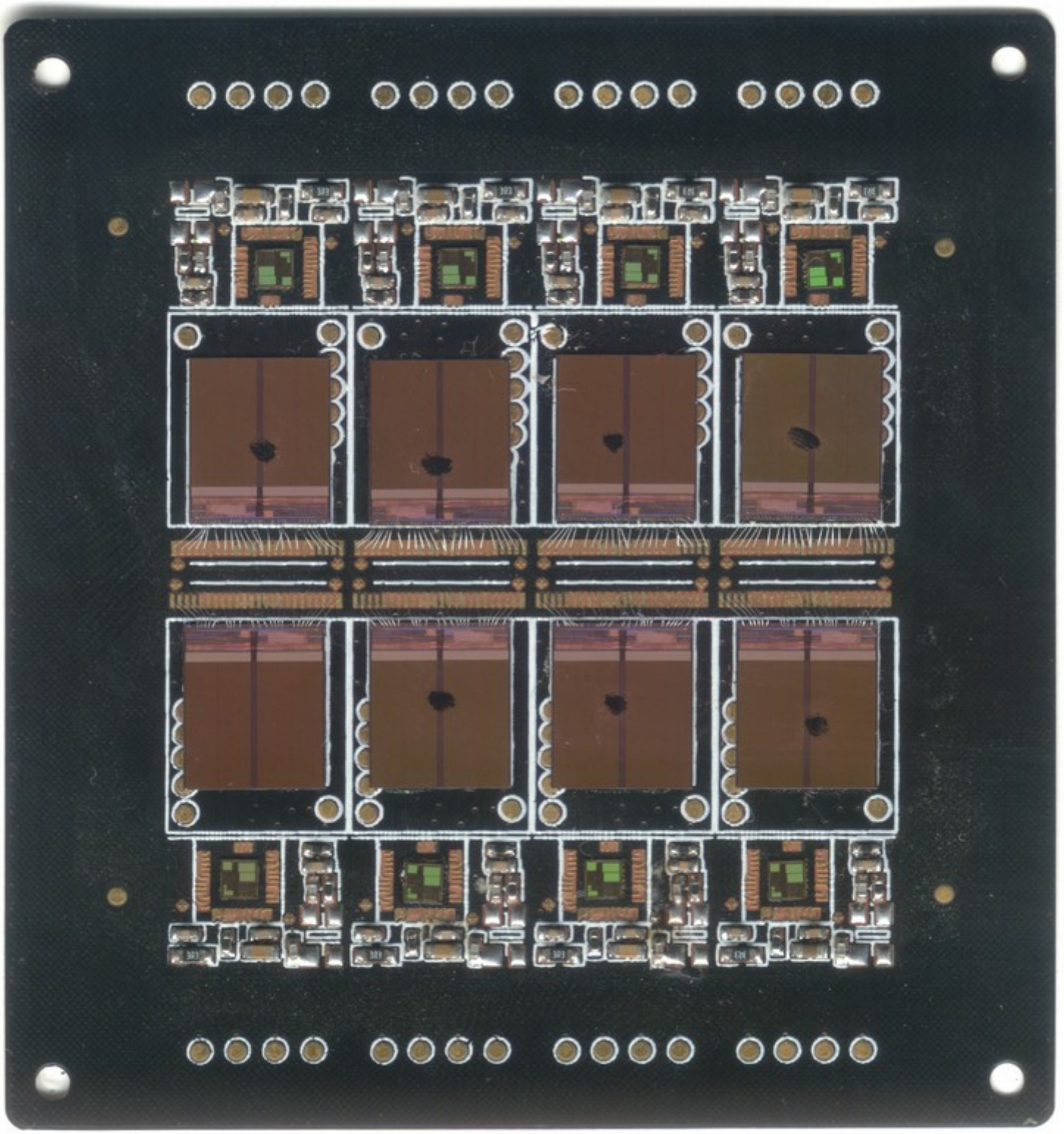
Monolithic USB Close-Ups

@BunnieStudios



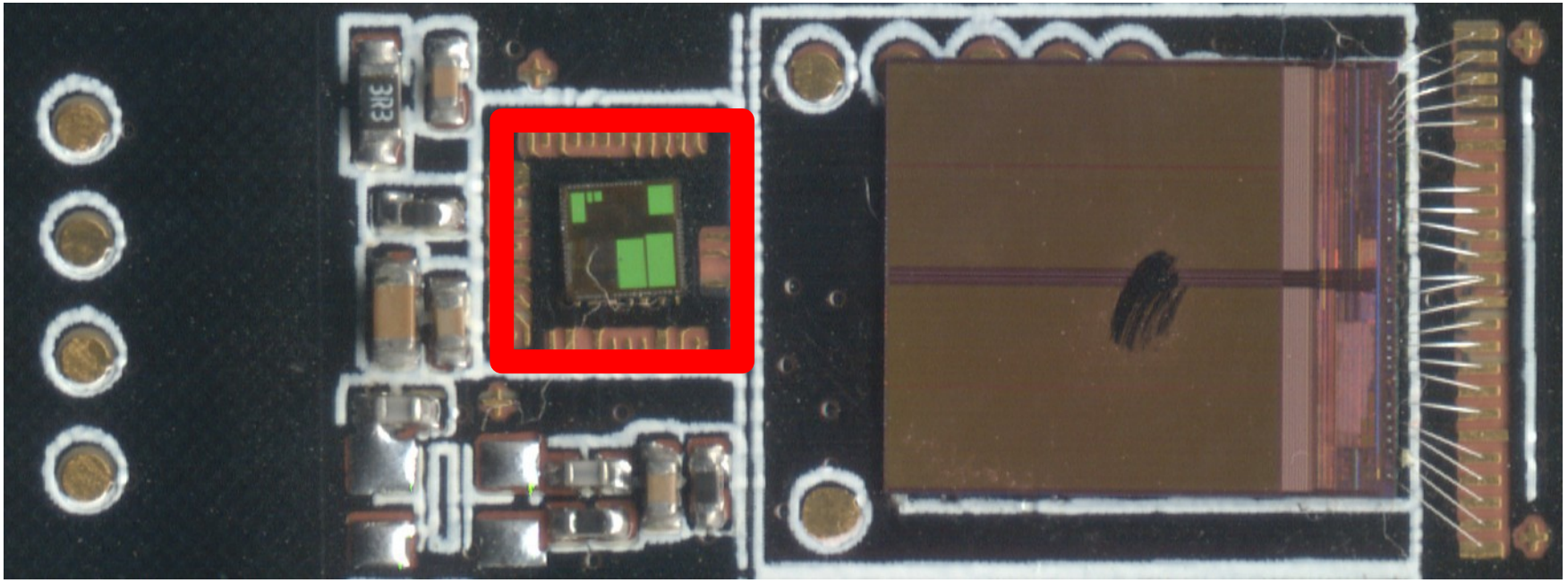
http://www.bunniestudios.com

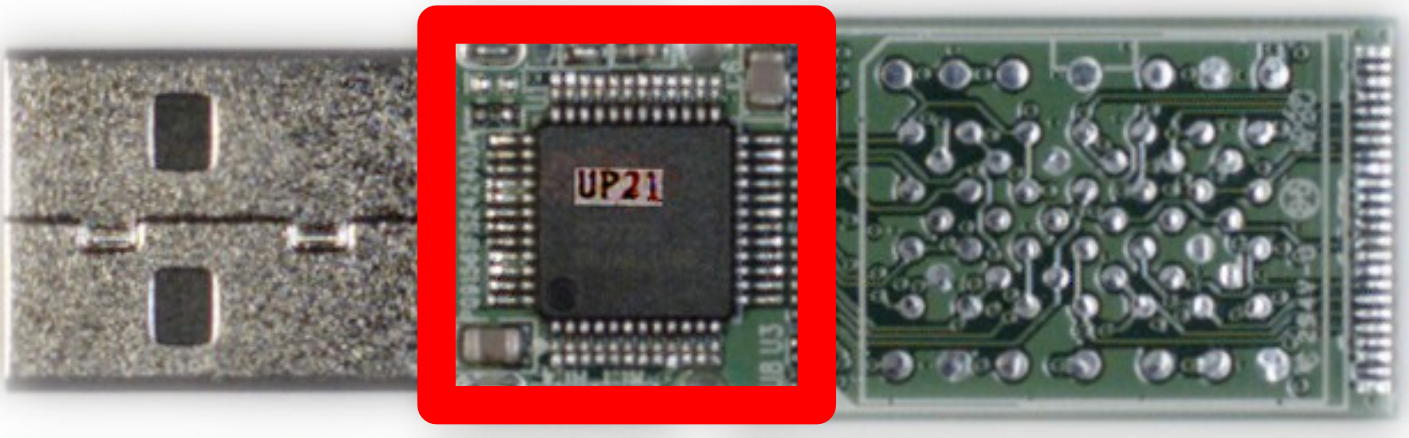
@BunnieStudios



http://www.bunniestudios.com

Monolithic v.s. PCB

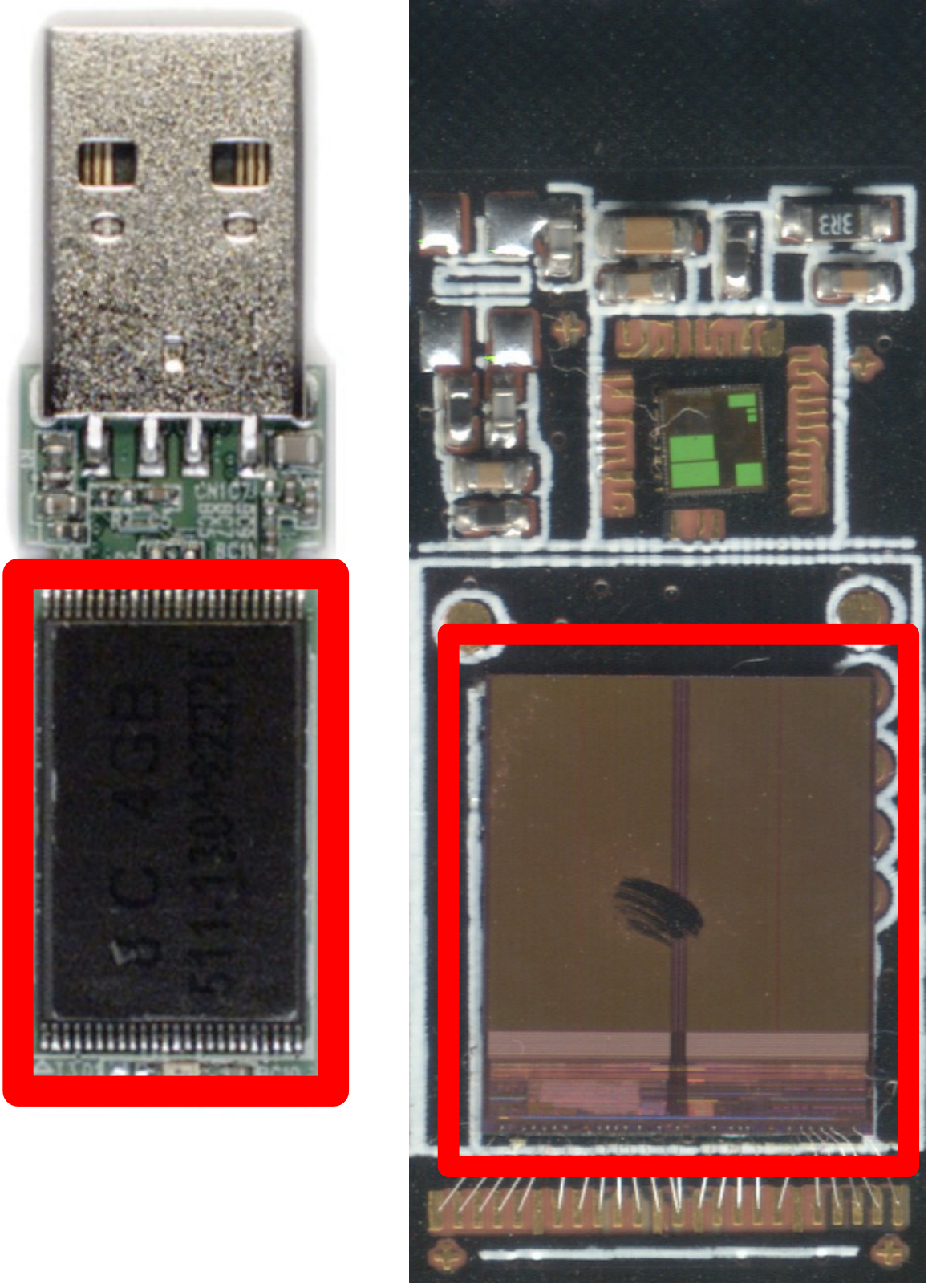




@BunnieStudios

http://www.bunniestudios.com

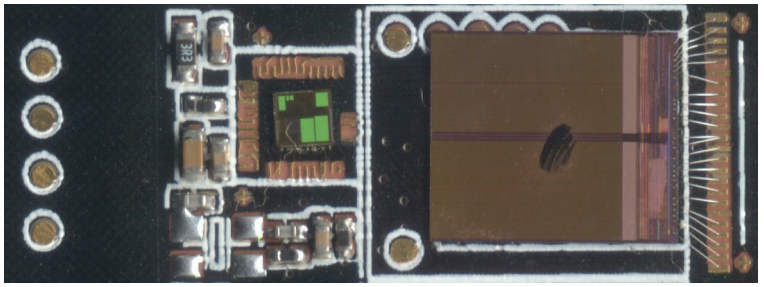
@BunnieStudios

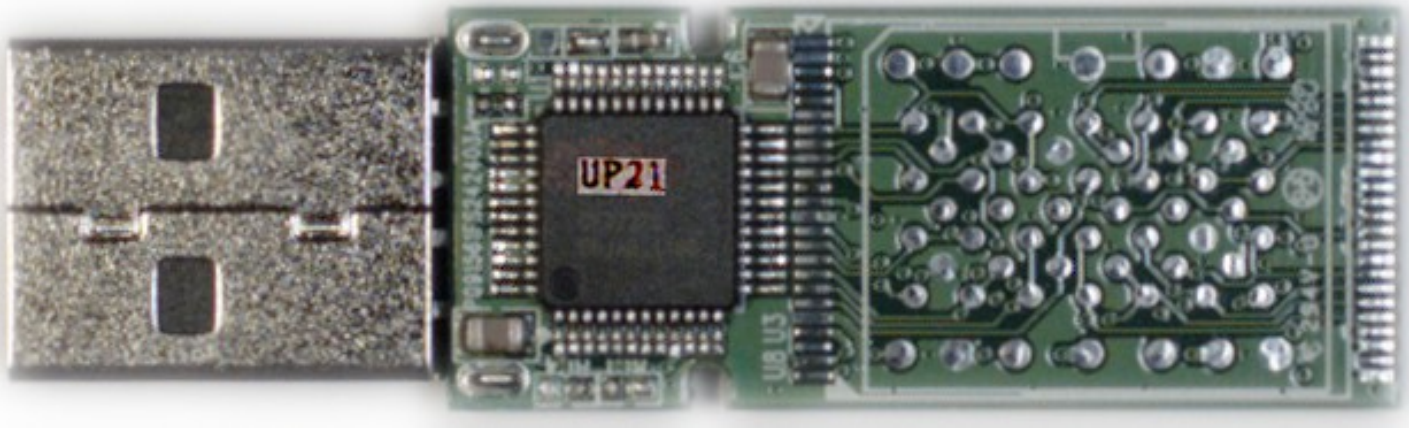


Monolithic v.s. PCB

http://www.bunniestudios.com

Monolithic v.s. PCB
(to scale)





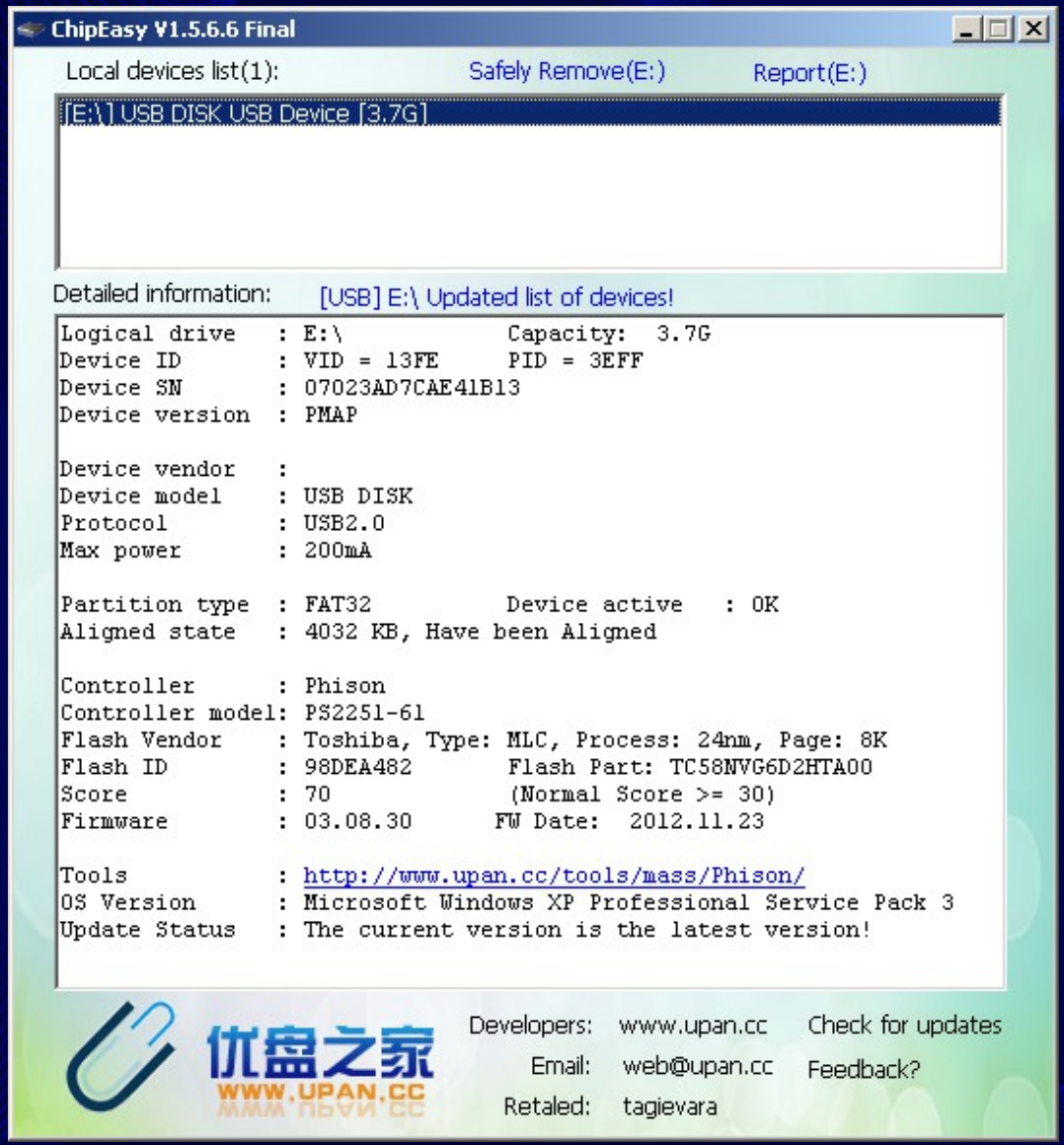
Visual Flash Controller ASIC Identification

- Destroys/mangles device housing
- Consumer packaging never mentions controllers
- OEMS use anything (Kingston)
- Monolithic drives are epoxied
- I don't have nitric acid + fume hood.

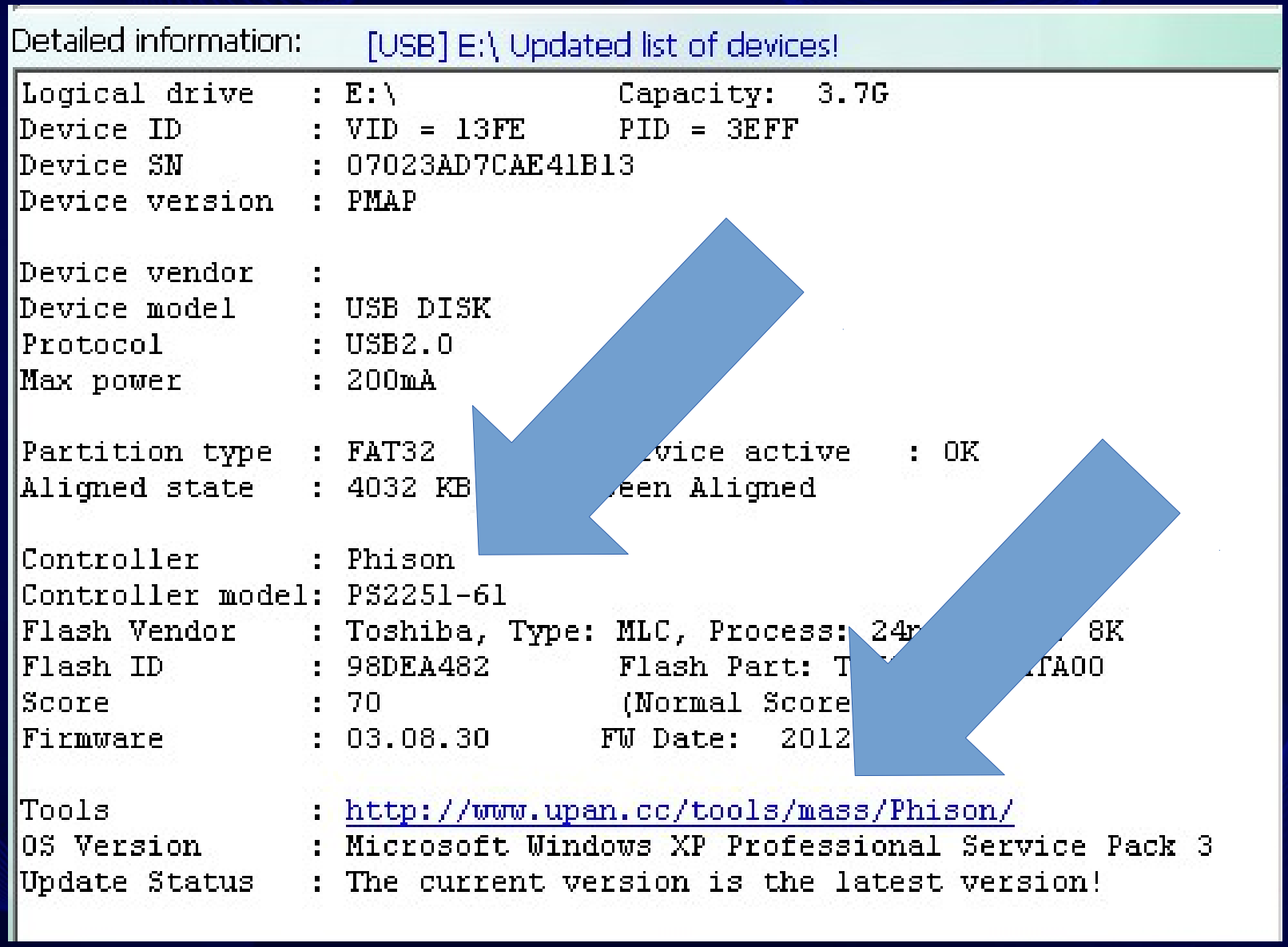
Software Flash Controller ASIC Identification

- OS sees what the ASIC wants it to
- USB PID:VID is *supposed* to be useful
- lsusb & friends are *useless*
- Need to talk to the ASIC directly
- No OS tools to talk to ASIC
- What software?

ChipEasy


ChipEasy V1.5.6.6 Final
Local devices list(1):
Safely Remove(E:)
Report(E:)
[E:\] USB DISK USB Device [3.7G]
Detailed information:
[USB] E:\ Updated list of devices!
Logical drive : E:\ Capacity: 3.7G
Device ID : VID = 13FE PID = 3EFF
Device SN : 07023AD7CAE41B13
Device version : PMAP
Device vendor :
Device model : USB DISK
Protocol : USB2.0
Max power : 200mA
Partition type : FAT32 Device active : OK
Aligned state : 4032 KB, Have been Aligned
Controller : Phison
Controller model: PS2251-61
Flash Vendor : Toshiba, Type: MLC, Process: 24nm, Page: 8K
Flash ID : 98DEA482 Flash Part: TC58NVG6D2HTA00
Score : 70 (Normal Score >= 30)
Firmware : 03.08.30 FW Date: 2012.11.23
Tools : http://www.upan.cc/tools/mass/Phison/
OS Version : Microsoft Windows XP Professional Service Pack 3
Update Status : The current version is the latest version!
优盘之家
WWW.UPAN.CC
Developers: www.upan.cc
Email: web@upan.cc
Retaled: tagievara
Check for updates
Feedback?

ChipEasy


Detailed information:
[USB] E:\ Updated list of devices!
Logical drive : E:\ Capacity: 3.7G
Device ID : VID = 13FE PID = 3EFF
Device SN : 07023AD7CAE41B13
Device version : PMAP
Device vendor :
Device model : USB DISK
Protocol : USB2.0
Max power : 200mA
Partition type : FAT32 vice active : OK
Aligned state : 4032 KB een Aligned
Controller : Phison
Controller model: PS2251-61
Flash Vendor : Toshiba, Type: MLC, Process: 24r 8K
Flash ID : 98DEA482 Flash Part: T TA00
Score : 70 (Normal Score
Firmware : 03.08.30 FW Date: 2012
Tools : http://www.upan.cc/tools/mass/Phison/
OS Version : Microsoft Windows XP Professional Service Pack 3
Update Status : The current version is the latest version!

Picking on Phison

- Taiwan based Flash controller ASIC manufacturer
- Controller interfaces: USB 1/2/3, SATA, IDE, eMMC, SD & more
- Core CPU: Intel 8051 (on-die)
- Hardware AES-256 (in some controllers)
- Multiple device "modes"

Flash ASIC-based Crypto…

1) Flash controllers do wear-leveling
2) Encryption key ***may*** be held in the ASIC, initially set during ASIC programming
3) LUNs (drives) can be hidden, locked w/ password AND encrypted
4) Flash drives have more space than you know

This is a forensics NIGHTMARE

PS2251 Series Flash Modes (Logical Units)

Mode #	LUN0	LUN1	LUN2
(common) 3	HDD		
7	HDD	HDD*	
8	HDD*‡	HDD‡	
14	HDD	HDD	CDROM
(common) 21	CD	HDD	
30	CD		
31	CD	HDD*	HDD
32	CD	CD	

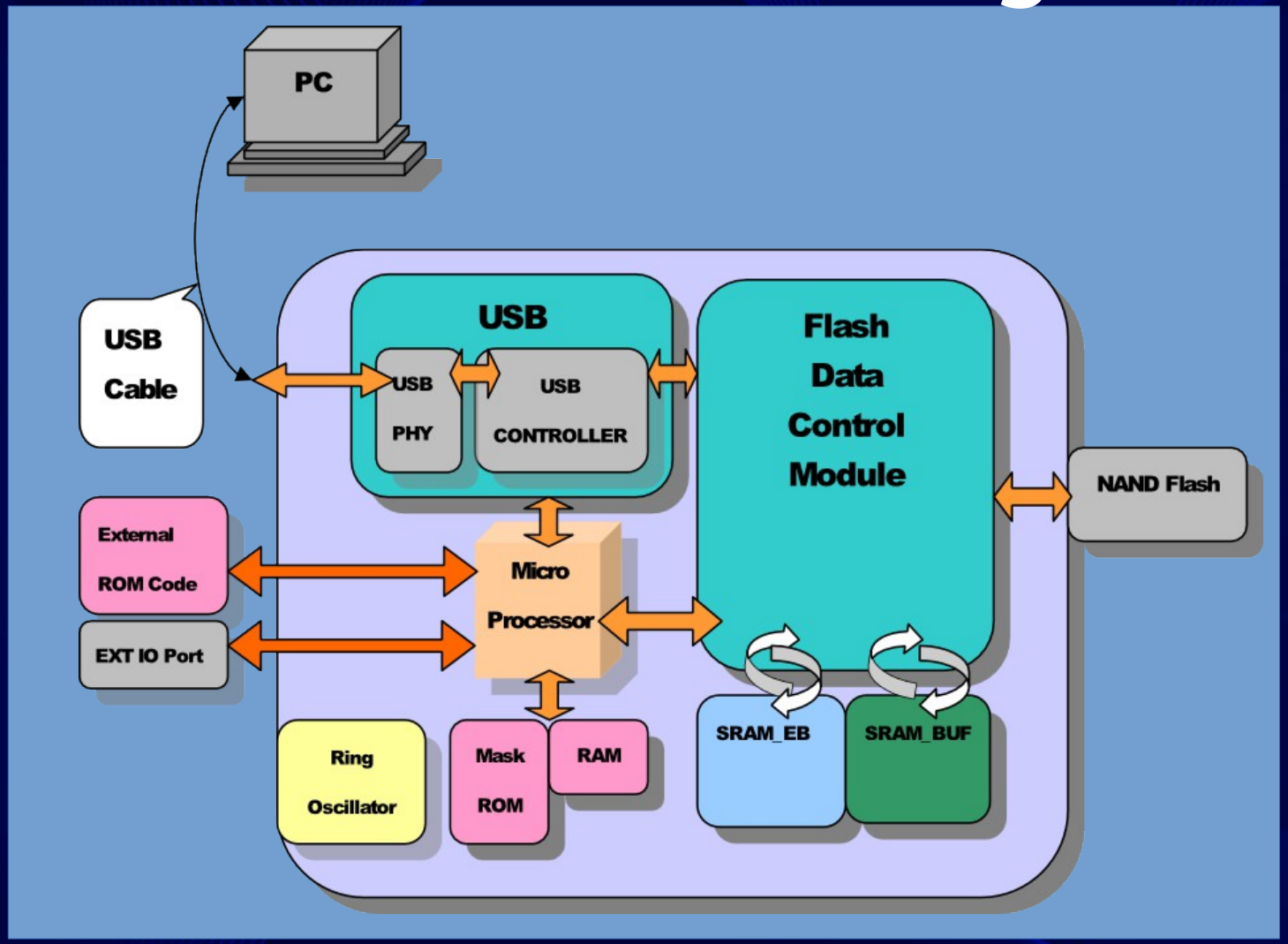
* LUN invisible until unlocked w/ app

‡ Only one LUN visible at a time

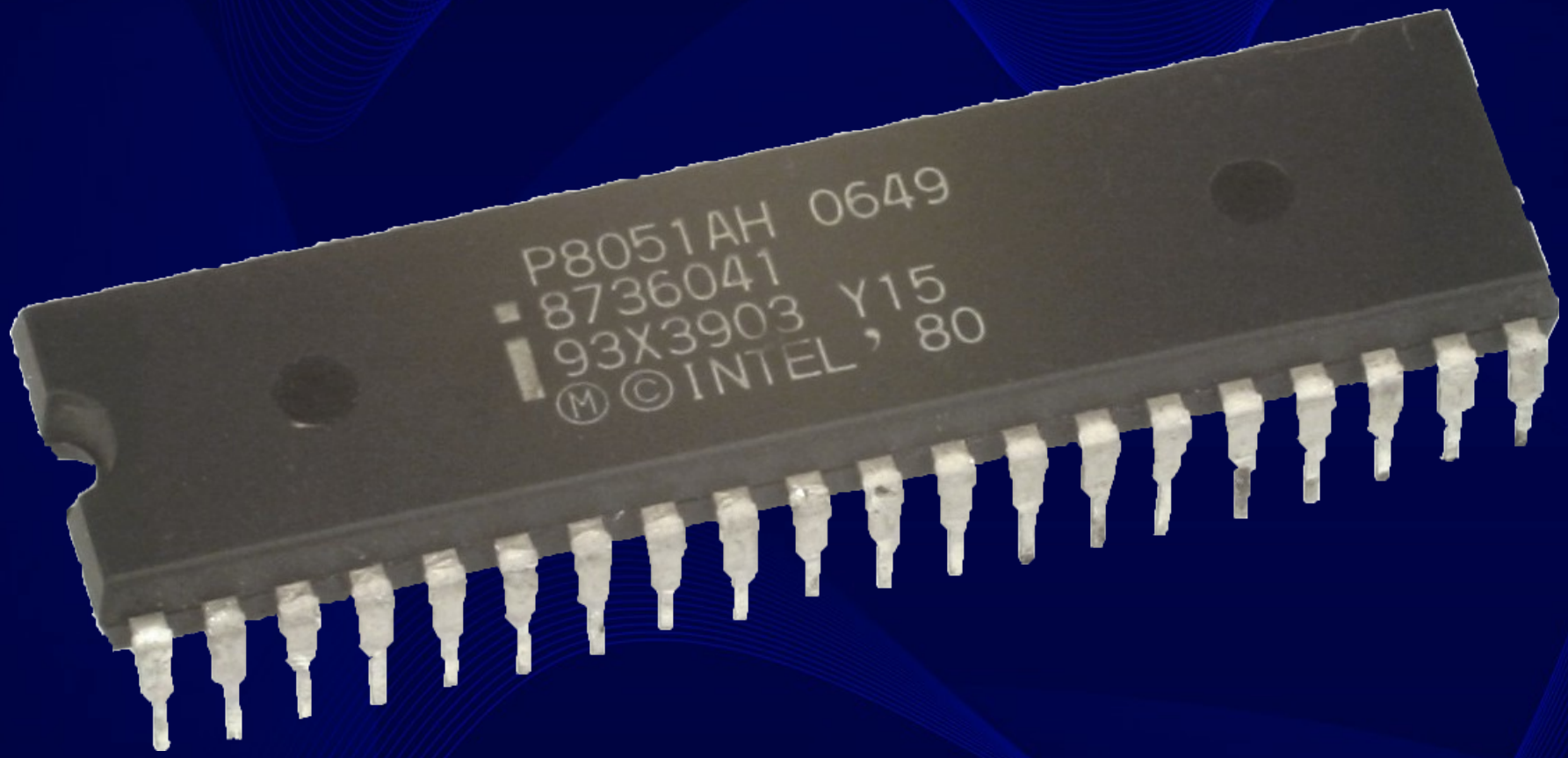
No more U3 drives!

- Mode 21 is “U3” like
- U3 drives are *dead* as of 2009 thanks to Microsoft & SanDisk
  - Superseded by “StartKey”
  - Appears to be related to “Windows 2 Go”
- Flash drives you already have most likely support mode 21.

PS2251 Block Diagram



Hello, Intel 8051

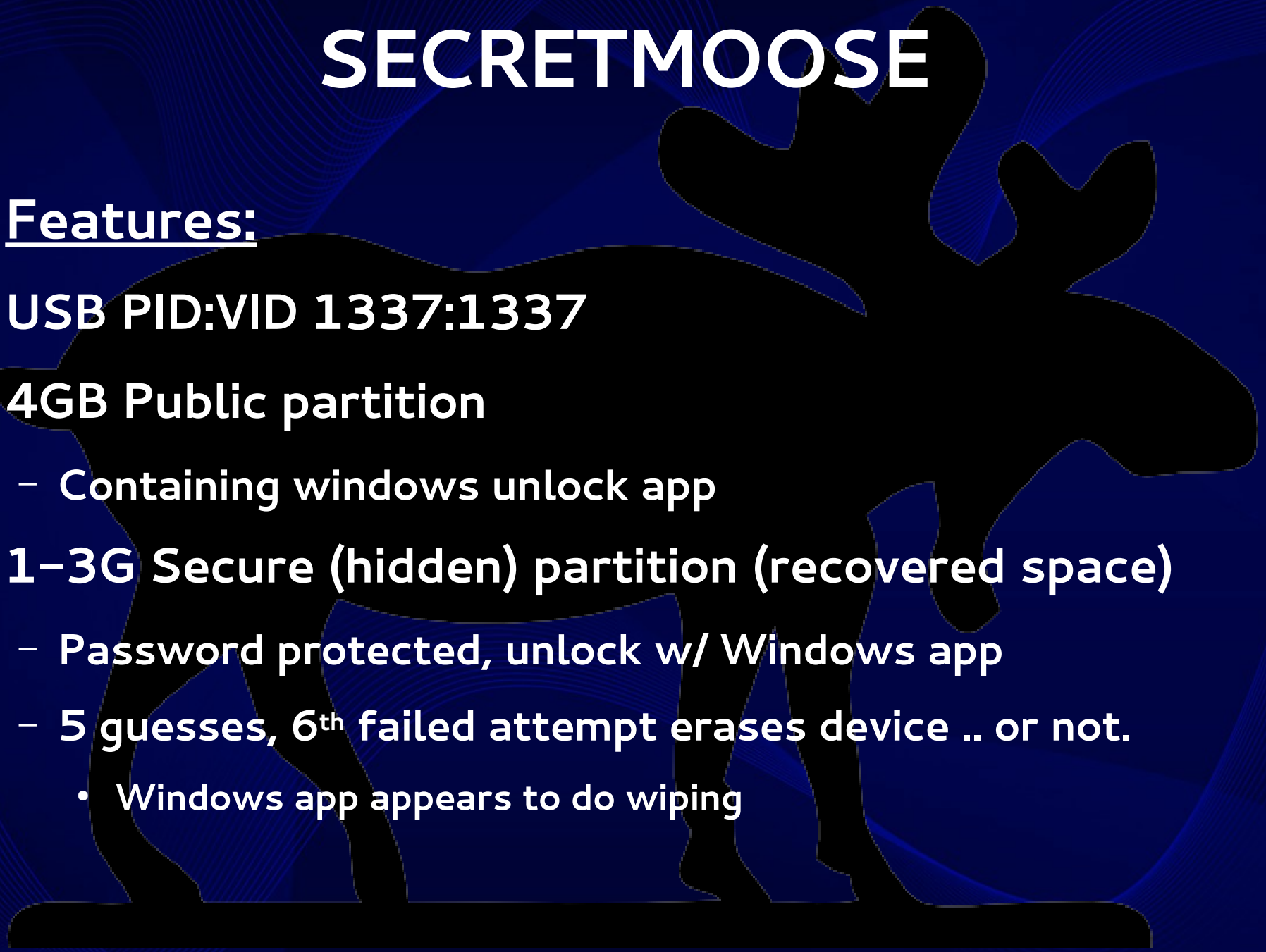


Bunnie & xobs @ 30C3
"SD Card Hacking"

- Re-purposing 8051 MCU inside SD cards
- Arbitrary code execution on controller in SD Cards
- Most likely will work with these flash drives too, similar controllers
- RE'd a controller, wrote a debugger!
- 8051 is an "IP" core – it's EVERYWHERE


MOOSEDRIVES
(NOT FOR SALE, SORRY)
4GB Flash
$5 Microcenter Brand
Phison 2251-61

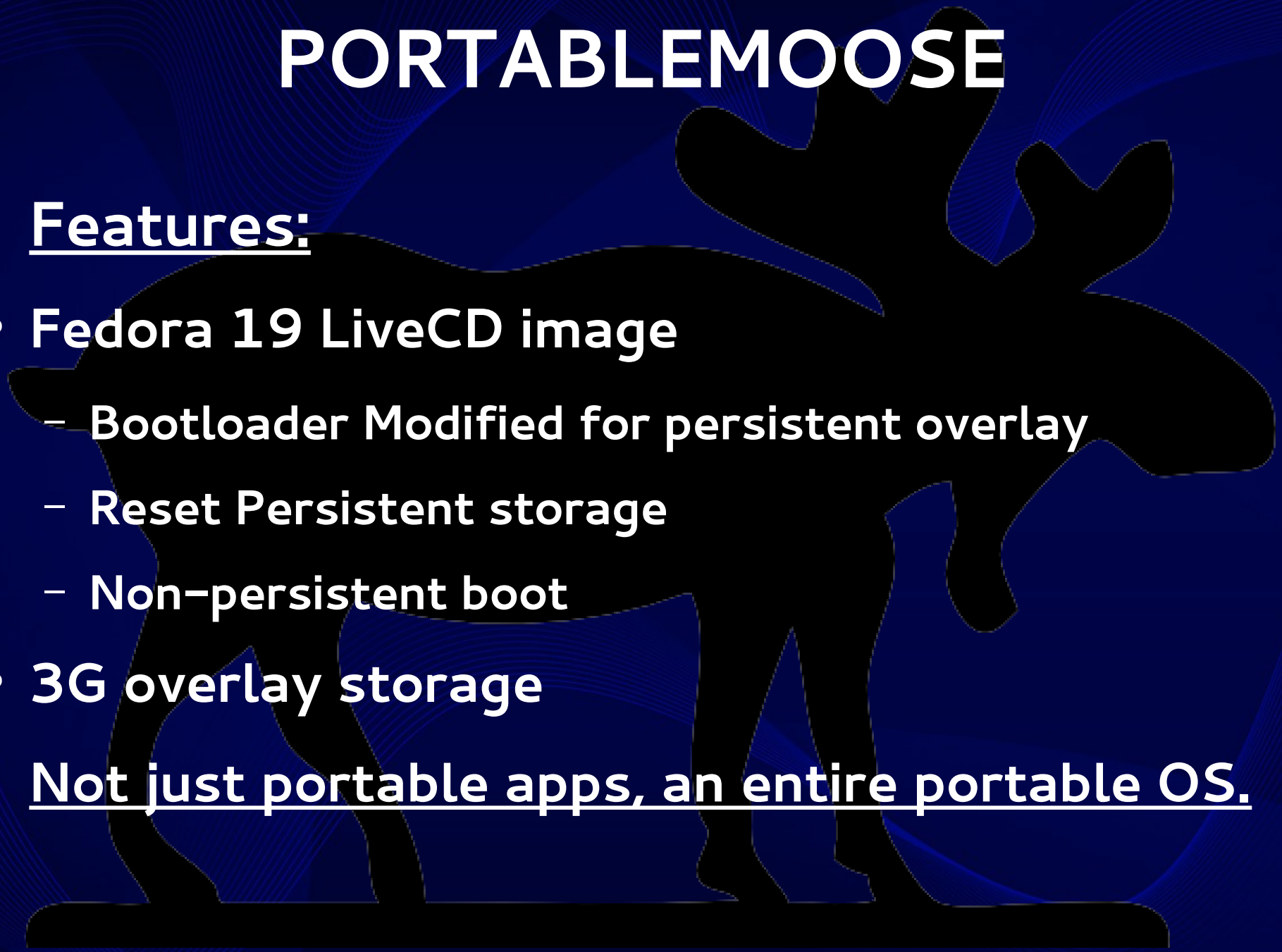
SECRETMOOSE



Features:

- USB PID:VID 1337:1337
- 4GB Public partition
  - Containing windows unlock app
- 1–3G Secure (hidden) partition (recovered space)
  - Password protected, unlock w/ Windows app
  - 5 guesses, 6th failed attempt erases device .. or not.
    - Windows app appears to do wiping

PORTABLEMOOSE

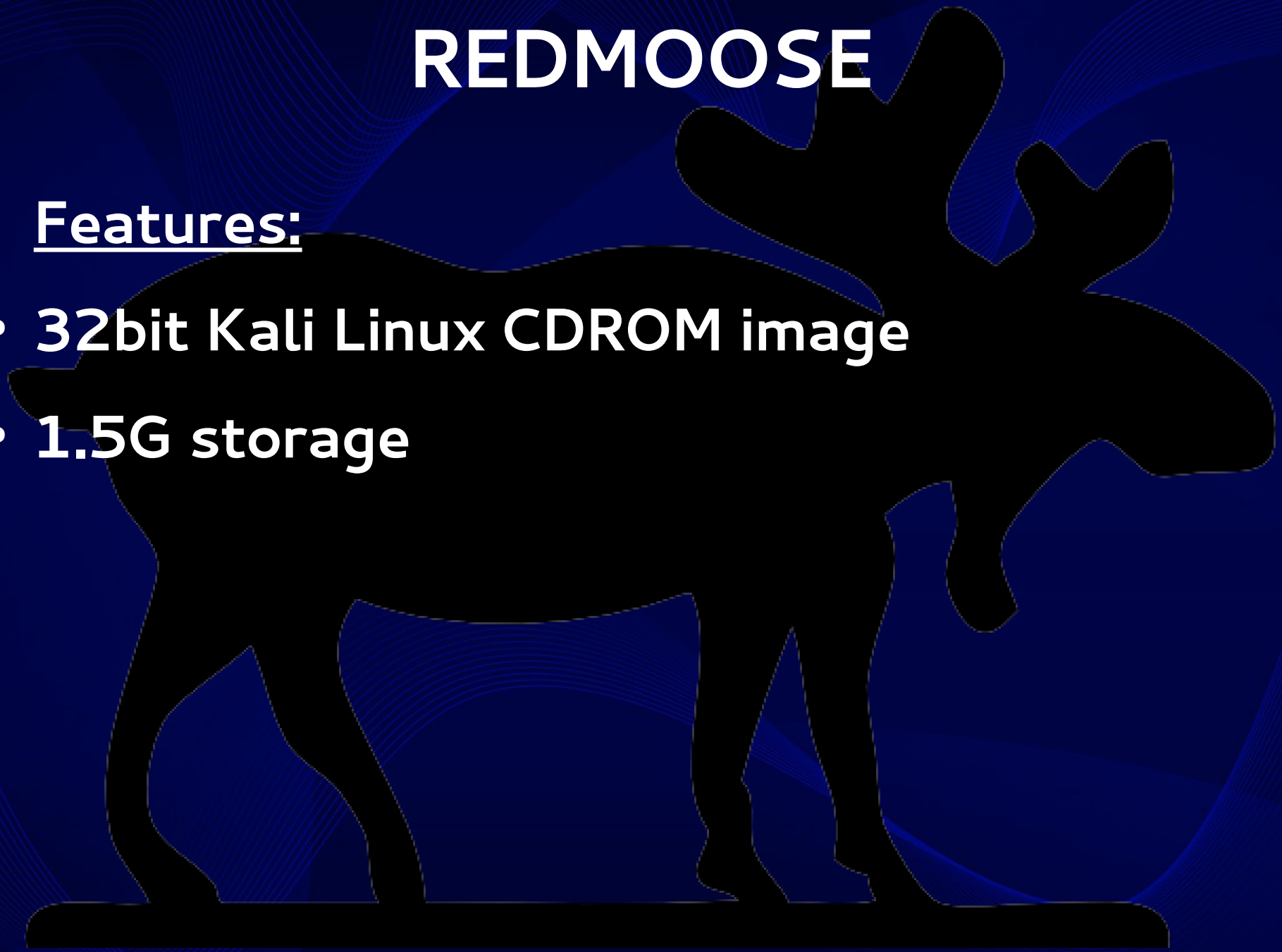


Features:

- Fedora 19 LiveCD image
  - Bootloader Modified for persistent overlay
  - Reset Persistent storage
  - Non-persistent boot
- 3G overlay storage

Not just portable apps, an entire portable OS.

REDMOOSE



Features:

- 32bit Kali Linux CDROM image
- 1.5G storage

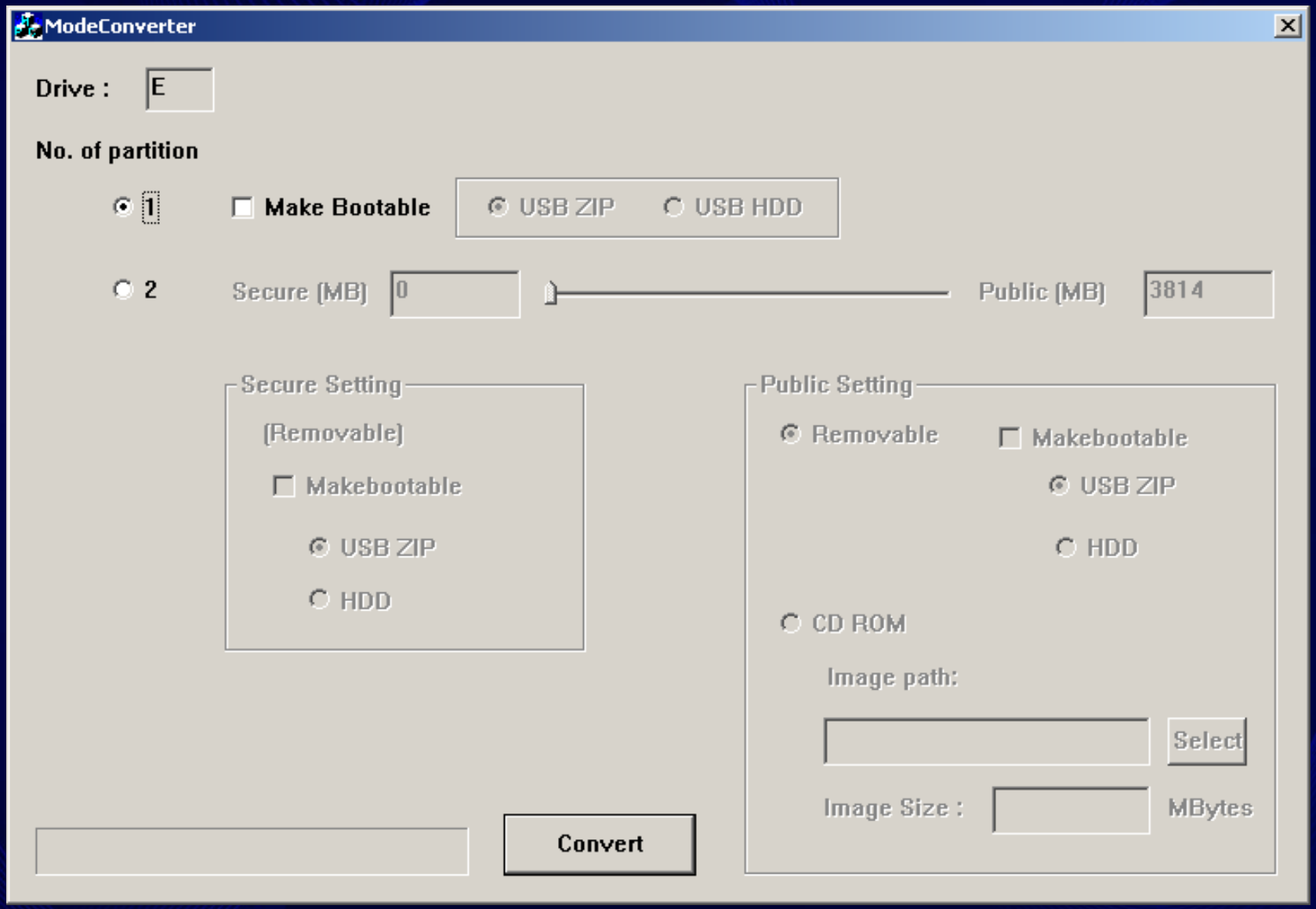
Which is for you?

- ISOSTICK
  - $99, uSD (up to 64g), “isosel” boot loader
- CDEMU
  - Open source project, still in development
- Regular thumb drives
  - $0 – $??
  - A little of your time + varying levels of “fun”

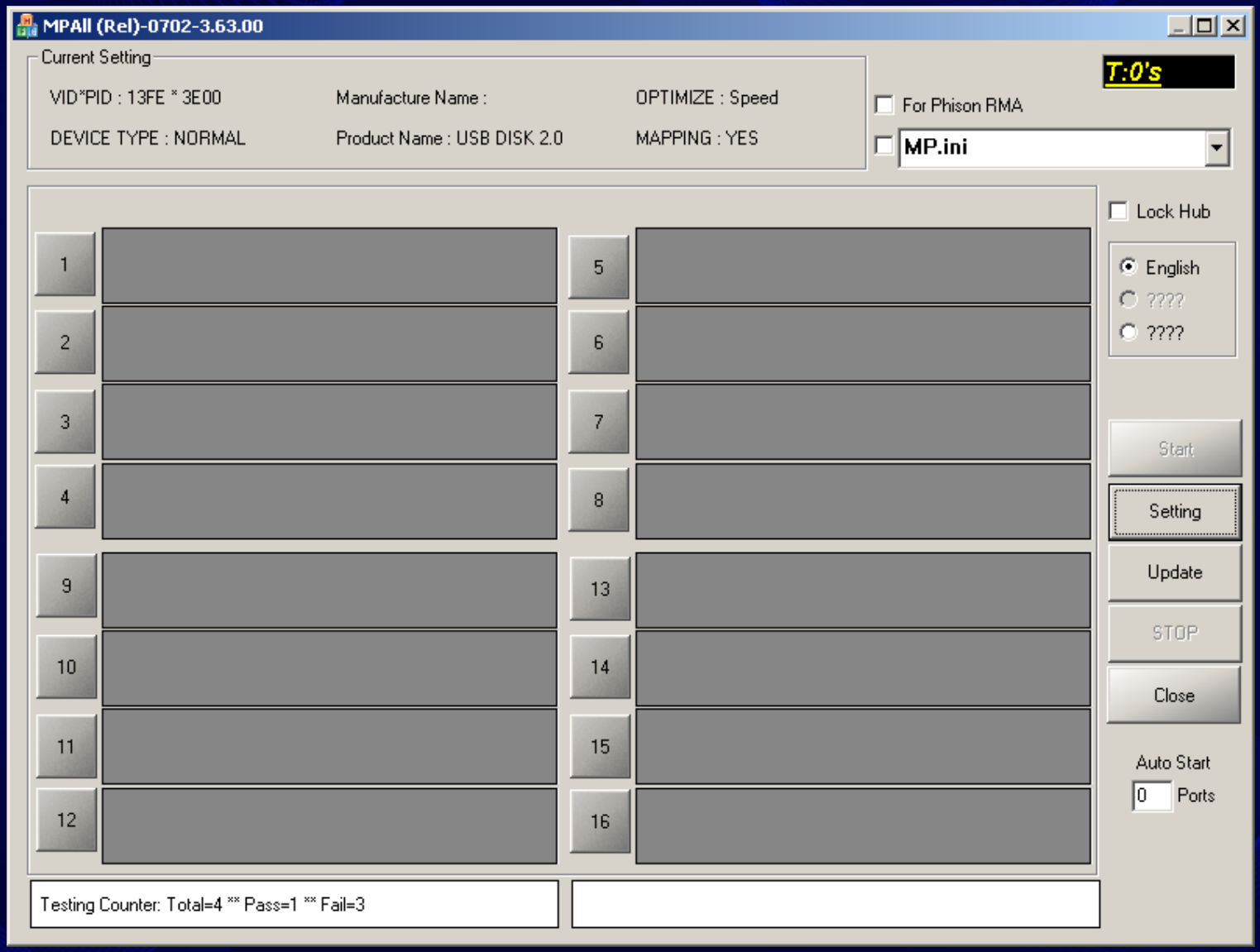
(Re)programming Phison Controllers

- Foolproof/Easy Mode:
  - Mode Converter
  - Switch between different modes easy
- Dangerous/Advanced:
  - MPAll
  - GetInfo utility bundled (more info than ChipEasy)
  - Change firmware, partitioning, USB identification, password lock, enable crypto (if supported)

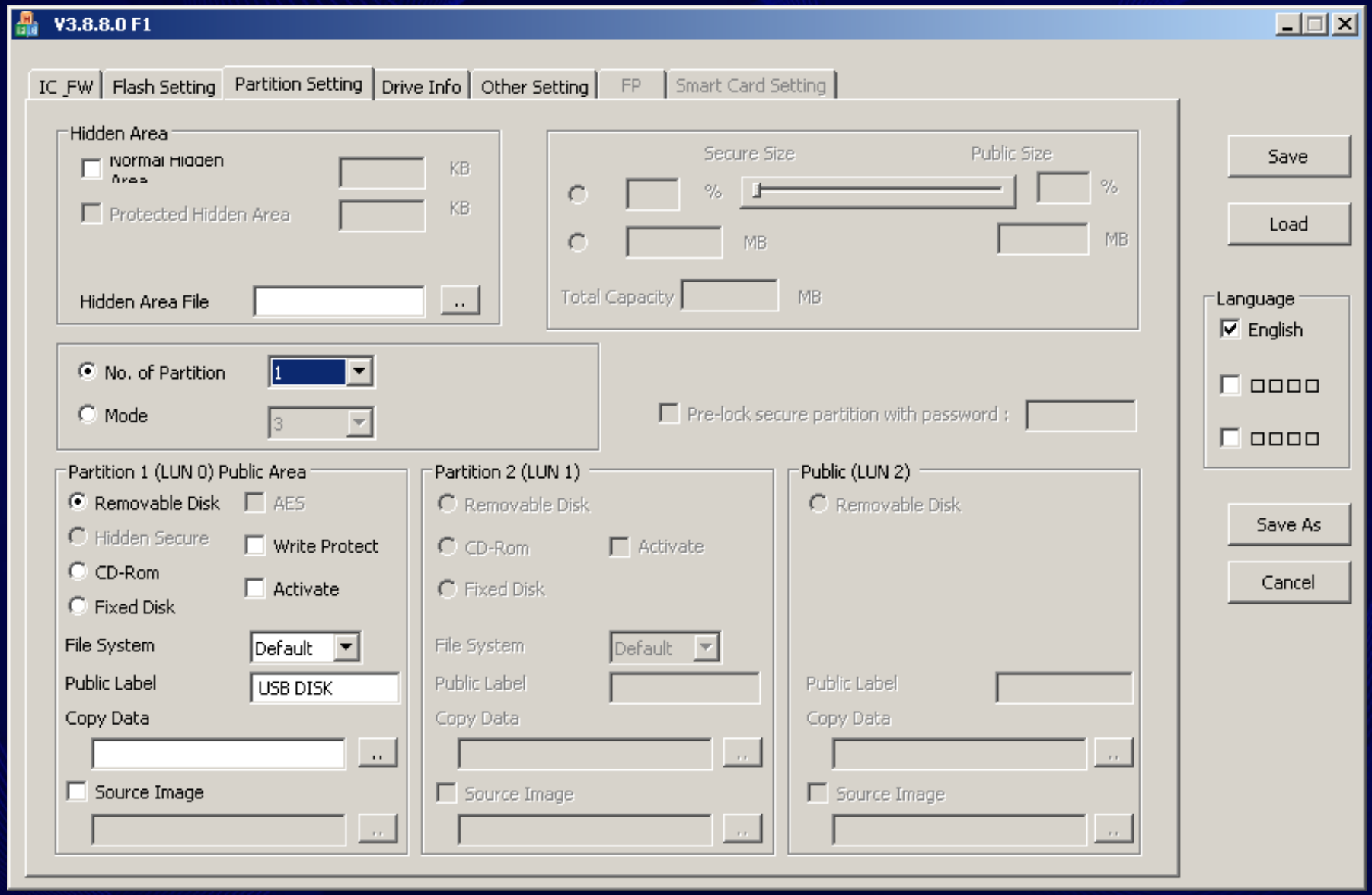
Phison ModeConverter

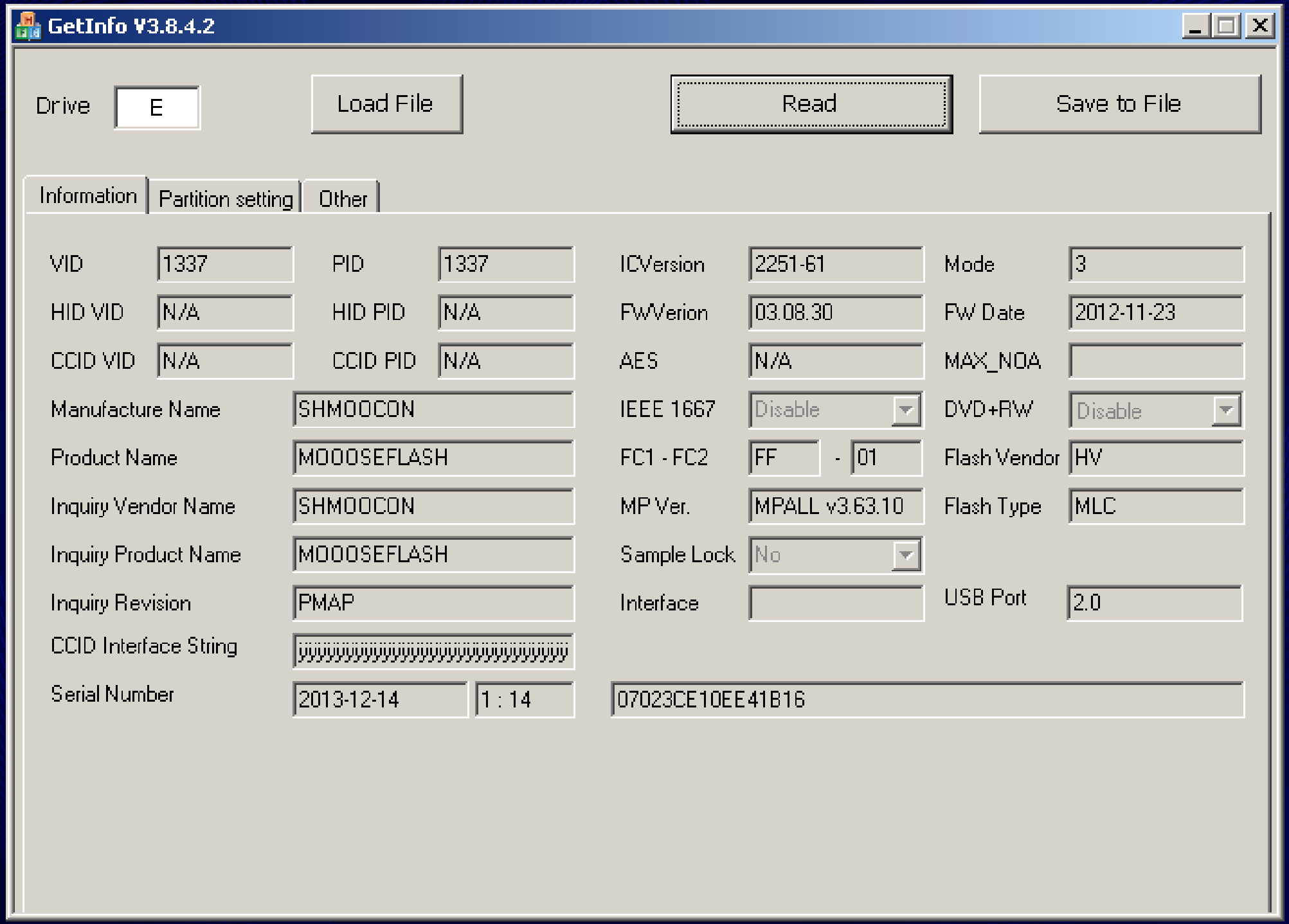


Phison MPAll



MPAll Partitioning (LUNs)




GetInfo V3.8.4.2
Drive
E
Load File
Read
Save to File
Information
Partition setting
Other
VID
1337
PID
1337
ICVersion
2251-61
Mode
3
HID VID
N/A
HID PID
N/A
FWVerion
03.08.30
FW Date
2012-11-23
CCID VID
N/A
CCID PID
N/A
AES
N/A
MAX_NOA
Manufacture Name
SHMOOCON
IEEE 1667
Disable
DVD+RW
Disable
Product Name
MOOOSEFLASH
FC1 - FC2
FF
-
01
Flash Vendor
HV
Inquiry Vendor Name
SHMOOCON
MP Ver.
MPALL v3.63.10
Flash Type
MLC
Inquiry Product Name
MOOOSEFLASH
Sample Lock
No
Inquiry Revision
PMAP
Interface
USB Port
2.0
CCID Interface String
Serial Number
2013-12-14
1 : 14
07023CE10EE41B16

Configurable Settings

- Drive Size
- Multi-LUN
- Device IDs & Strings
- Emulate CDROMs
- Serial Number
- # of ECC bits
- Set LUNs R/O
- LUN PW Protect
- Turn LED on/off
- Memory voltages
- Reformat (recover)
- Memory Timing

Phison MPAll Troubleshooting

- Use ChipEasy Flash ID to help
- Try the latest version of MPAll
- Be prepared to brick drives! (until you learn)
- Find Controller Firmware updates
- IDBLK_TIMING.dll updates – Updated Flash ID & Timing params
- Tripple check Flash ID & Timings are correct


GOOD IDEA
BAD IDEA

UnRAID, by Lime Technology

- Slackware based commercial NAS solution
- Different Tiers for supported # of HDD:
  - Free: <= 3, Plus: <= 7, Pro: <= 24
- Cost per Server:
  - Free: $0, Plus: $69, Pro: $119
- Licensing Method:
  - 27 character USB Flash drive GUID

Not so globally unique

lime-technology.com/registration-keys/

- Example GUID:
  - 058F-6387-0000-0000B65F1E82
  - This was an Alcor Flash Drive s/n: B65F1E82
- www.linux-usb.org/usb.ids
  - VID 058F: Alcor Micro Corp
  - PID 6387: Flash Drive

Cloning an unRAID Registration Key

1) Set USB VID and PID to match
2) Set Serial number to match
3) Win!

Please use a real hardware security token like the Aladdin HASP.

Looking for a HW USB Sniffer?

- See Dominic's Talk tomorrow:
  - An Open and Affordable USB Man in the Middle device
- No public documentation on programming flash controllers
- Windows + USBpcap + Wireshark insufficient :(
- No Linux support
  - usb_modeswitch has no idea about these controllers

Similar Work / Research

- 2013: Bunnie & xobs
  - 30C3 – SD Card Hacking

    http://www.bunniestudios.com/blog/?p=3554
- 2013: Bunnie
  - Where USB memory sticks are born

    http://www.bunniestudios.com/blog/?p=2946
- 2011: Wesley McGrew @McGRewSecurity
  - Hacking U3 drives
    http://mcgrewsecurity.com/pub/hackingu3

Similar Work / Research

- 2010: Digital Forensics Research Center – Korea
  - Secure USB Bypassing Tool
    http://www.dfrws.org/2010/proceedings/bang.pdf
- 2010: SySS
  - PW protected flash drives unlocked w/ single command
  - http://www.darkreading.com/security/news/222200174
- 2008: Russel Butturini / TCSTool
  - Incident Response U3 Switchblade

Links & Contact

ChipEasy: Google “Chipeasy English”

flashboot.ru

usbdev.ru

usb-fix.blogspot.com

upan.cc

xabean 

 warewolf

richard@richardharman.com