



**Insyde Software & UEFI:
A Commitment to Next Generation Firmware**

**UEFI Plugfest
Nanjing, P.R.C.
June, 2007**

Agenda

- Insyde Software Overview
- UEFI Compatibility Now and for the Future
- A Framework Approach to Next-Gen BIOS
- InsydeDIY – A New Solution for EFI/UEFI for Embedded Systems
- Conclusion

Insyde Software

- Develops, deploys and supports modern BIOS replacement firmware that is based on the EFI Framework and UEFI 2.0
- Founded September 1998 via the acquisition of SystemSoft's platform products division; Offices in China, Taiwan, Korea, & U.S.
- Longstanding Intel partner, ICAP portfolio company
- Target markets: Server, Desktop, Mobile and Embedded
- Insyde Software and InsydeH2O products:
 - ▶ Helps you Stay Current with new technology
 - ▶ Helps you Save Time in your product development
 - ▶ Helps you Save Money on your firmware development



Insyde offers Products & Services

Source Code and Tools

H2O source code licensed one time, plus additional modules (new CPUs, chipsets, etc)

Typically, new annual source fees
Source code Tools, eg. H2ODDT

Training

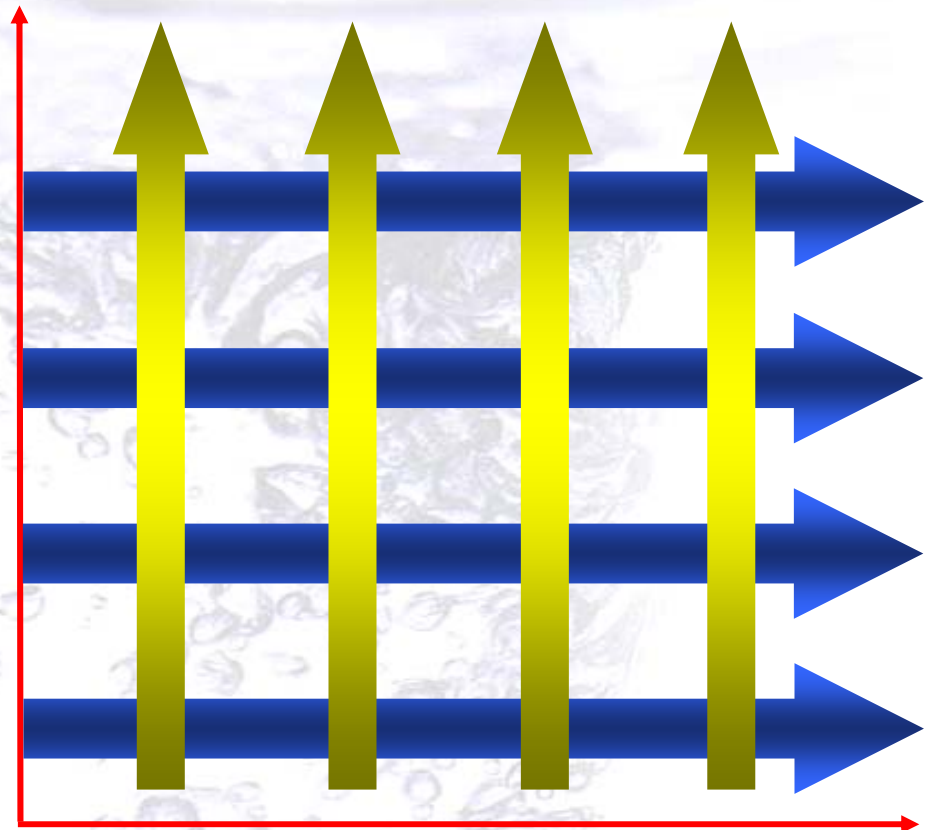
Multiple choices available, depending on needs

Customization

On project basis or retainer

InsydeH₂O Distribution

License fees for object code



**Mobile
Edition**

**Desktop
Edition**

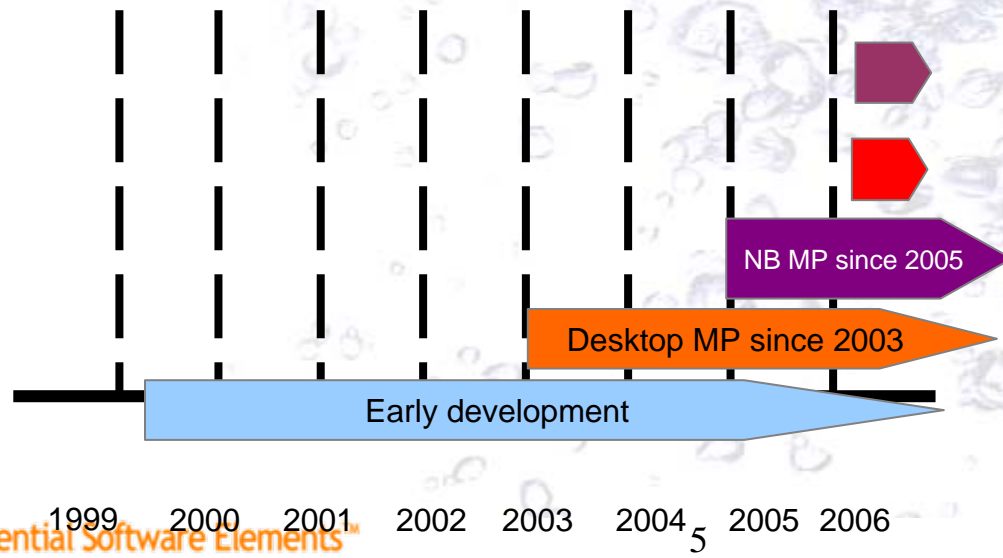
**Embedded
Edition**

**Server
Edition**



Recap of Insyde InsydeH2O Shipping status

- Over 5 years development experience on this technology
- Started shipping EFI products with H2O Desktop in 2003
- Started shipping EFI products with H2O Notebook in 2005
- Non-Intel chipsets supported in H2O/ shipping since Q1'06
- UEFI 2.0 ready in Q4 of 2006



Insyde H2O™ Customers and Partners



Shipping EFI Framework products since 2003

And more.....



Insyde Software & The UEFI Forum

- Insyde Software is 1 of 11 original Promoter companies that chartered the UEFI Forum
- Active at UEFI Board level and numerous working groups:
 - PIWG – Platform Initialization Working Group
 - USWG – UEFI OS Interface Spec
 - UTWG – UEFI Testing Working Group
 - ICWG – Industry Communications Working Group
- Active Supporter and implementer of TPM specifications from TCG

UEFI Compatibility

- Historic sources of this architecture
 - EFI 1.1 from Intel
 - Framework – full platform init and implementation of EFI 1.1
- Two UEFI Specifications
 - UEFI Specification – Interface presented to OS Boot and Runtime
 - Version 2.0 is current (published Jan '06)
 - Version 2.1 in development (published Jan '07)
 - UEFI PI Specification – The software structure that contains and supports chipset modules
 - Version 1.0 in development (published Nov '06)
 - Next portion of PI Spec is expected later this year



InsydeH2O Compatibility with UEFI 2.0

- InsydeH2O Supports UEFI 2.0 Spec
 - Native UEFI 64-bit Boot
 - GOP – advanced EFI video init
 - Dozens of improvements in USB, Networking, other
- Under development are key components that include improved User Interfaces to guide end users
- InsydeH2O supports PI Spec 1.0
 - Forms the basis of our collaboration with silicon suppliers:
 - » Intel – CPU and Chipset
 - » AMD – CPU and Chipset
 - » nVidia, SIS and others

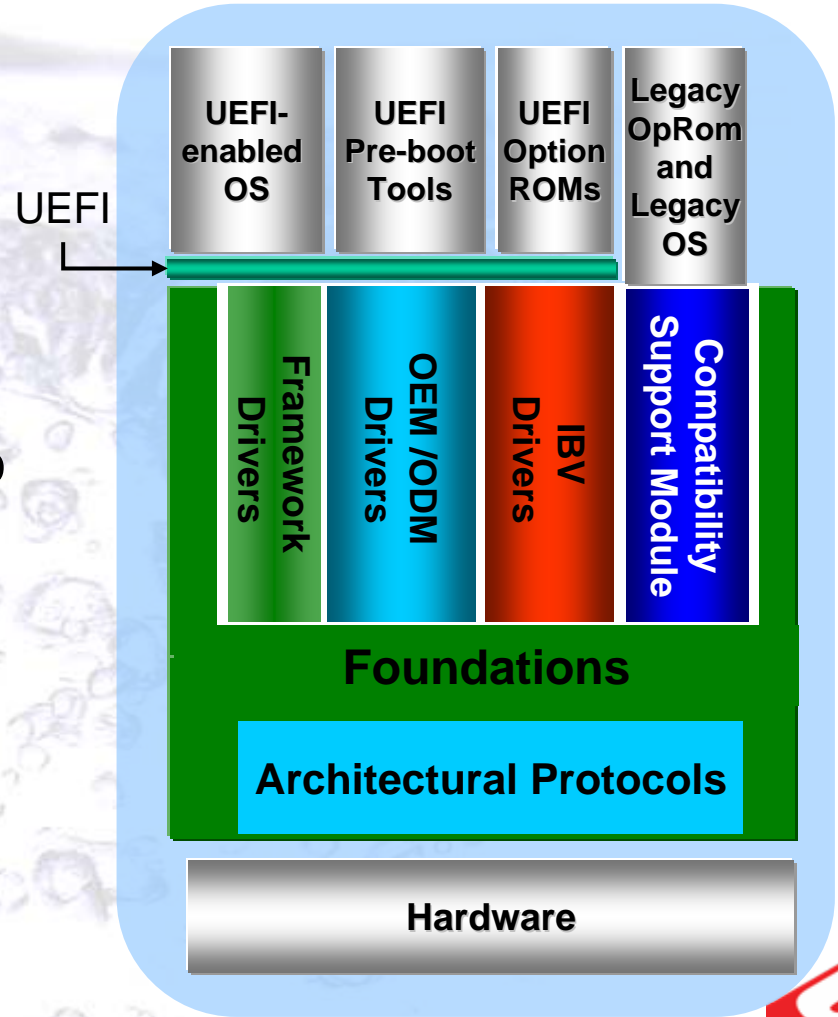
UEFI and Framework Basics

- Framework and UEFI PI
 - Initialize the CPU
 - Host the chipset modules which bring up devices and DRAM
 - Support Boot decision logic and other platform policy
 - Exposes UEFI Boot Services and Runtime Services
- EFI 1.1 and UEFI 2.0
 - Services for use by boot loaders and pre-boot application
 - Run-time services for use by OS after boot
- Framework later stages == UEFI boot services



CSM Overview

- CSM meshes Legacy Bios and Framework code to boot Legacy OS and load traditional OpROMs
- Simulate traditional INTs to load traditional OpROMs
- Update traditional tables
- Boot to traditional OS



Key CSM Functionality

- EFI Compatibility Support Module code initialization
- Traditional OpROMs dispatch
- Discovering devices and update traditional tables
- Boot OS
- Thunk and reverse thunk code
- Runtime traditional code provided by a IBV



Elements of UEFI Specification

- App is passed a pointer to UEFI System table with pointers to data and routines for:
 - Console I/O
 - Table of Required 'Run time' services
 - Table of Required 'Boot' Services
- Boot Services functions include routines for
 - Priority control, Memory allocation, mem copy, Event notification
 - Install and find, open and close, protocols and handles
 - Load Images for various devices, connect drivers to devices



More Elements of UEFI Specification

- Runtime Services Table includes routines for
 - Time, and mono counts
 - Virtual Memory remap after boot
 - NV Variables, get and set and query info
 - Pass capsules to the firmware
- A population of protocols which support devices needed for boot including
 - Driver load, connect, start and stop



Some of the Devices Supported by UEFI 2.0-Defined Protocols

- PCI Bridge and Device control
- Console, Keyboard, Mouse, Serial, USB
- Video display
- Disks including mag and optical, with partitions file system
- A new disk partitioning scheme GPT without legacy limits
- SCSI, iSCSI, SAS, SCSI Tape
- Complete Network stack with TCP/IP
- Security tools including hashing



Where Do UEFI Drivers Come From

- Generic drivers in your IBV Vendors library
- Chipset Devices from you Chipset vendor
- From the manufacturer of onboard devices and added to your build in either source or binary form
- What about plug-in cards?
 - Driver can be added to boot disk
 - New Option ROM Format (EBC) with Byte code interpreted works with any CPU or CPU Mode



Pre-boot Applications

- A EFI-native OS boot loader is a pre-boot application
- EFI Shell is a pre-boot application
- Many other applications are possible
 - diagnostics, provisioning and more
- Setup and Boot Manager are pre-boot applications that are typically built into BDS module
- Possible to go into application, execute, and come back to BDS to allow another choice
- Process ends when a successful boot loader call ExitBootServices()
 - Closes Down Boot Services and only Runtime Services Remain



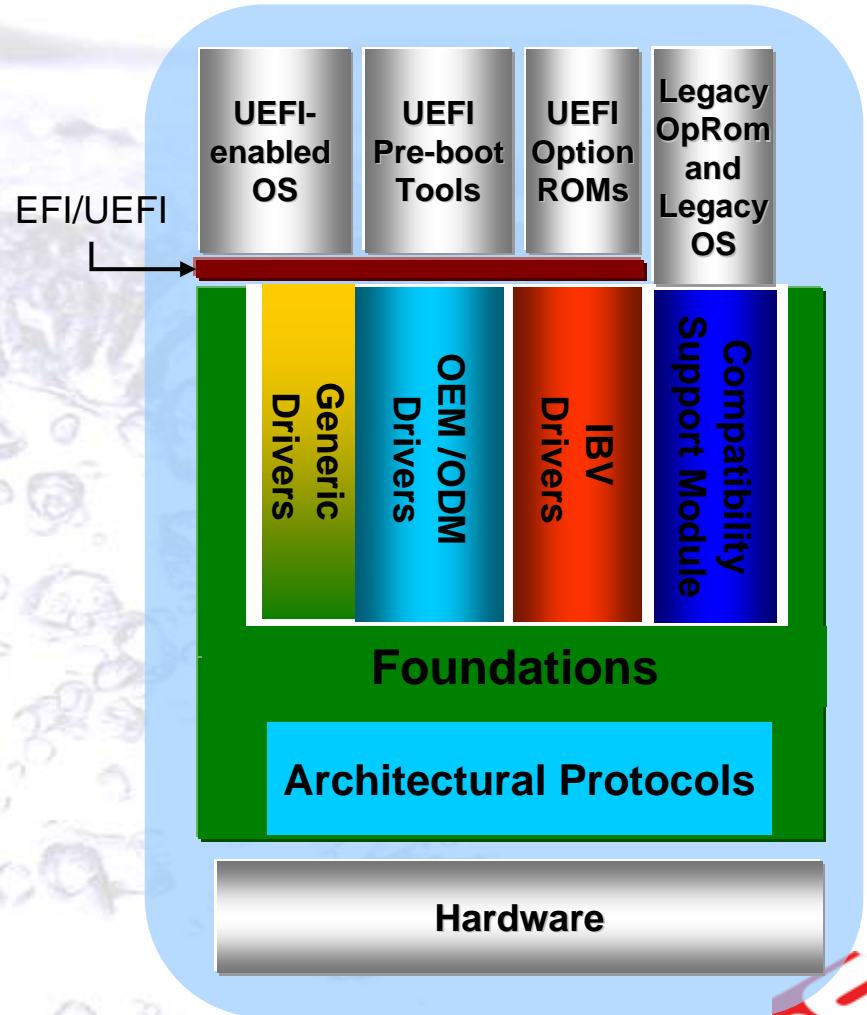
Insyde Software Solutions

InsydeH2O™ and InsydeDIY™



What is the Framework?

- New architecture of firmware
- Open Source Foundation code -“H”
- Silicon specific “PI” code
- Base drivers for platform
- SKU specific drivers
- IBV value add
- UEFI Compliance
- Legacy OS support



UEFI Framework Speeds New Technology

- Intel's plan for enabling new platforms is with Framework
 - ▶ CPU drivers, chipset drivers
 - ▶ CSI
 - ▶ *T Technologies (AMT, VT, EIT, TXT, future *Ts)
- Microsoft no longer committed to provide all features for Legacy Boot. Some features may only be enabled with UEFI
- Update of Vista will use UEFI boot

Insyde's Pure Framework is the quickest way to get support for future technologies



The Key Benefits of Framework

- Vendor not dependent on one BIOS/Firmware company or proprietary code base
- Vendor can create more efficient engineering teams
- Code developed once can be shared among Vendor's Business Units – same source code!
- Vendor can leverage pre-boot environment to drive product innovation

Derive real value & lower cost from the UEFI Framework

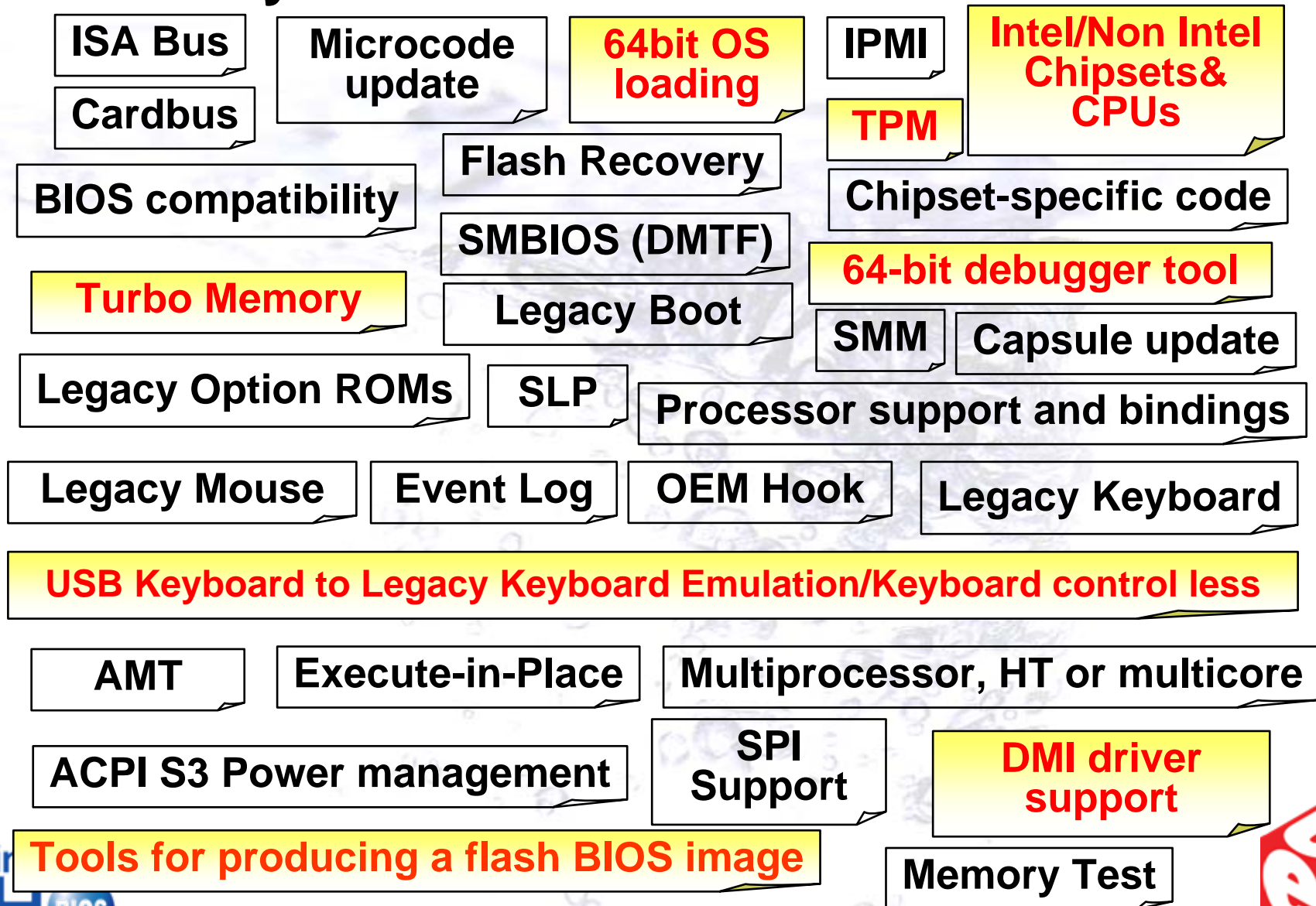
InsydeH2O – Far Beyond Intel Framework

- Production Quality Enhancements
- CSM – Compatibility Support Module
- Source-level Software Debug Tool
- Power Management
- USB Legacy
- EFI-based Setup
- VROM™ Technology
- Pre-boot Applications
- Full Coverage Training Materials from Level I to Level V
- Wide Range Chipsets /CPUs Supporting

Why leading OEMs/ODMs Select InsydeH2O



Insyde's Add-on Value to Framework



H2ODDT – Debug Tool

The screenshot shows the ISDebug - Intel865 debugger interface. The CPU window displays the following register values:

Register	Value
EAX	00000000
ECX	0EEC5DE0
EDX	0EEC6924
EBP	0EEFB4D4
ESI	000000DA
EDI	0DEE0140
ESP	0EEFB4B4
EIP	0DEDF2E4
CS	0010
SS	0018
DS	0018
ES	0018
FS	0018
GS	0018
NU UP DI PL	
NZ AC PE NC	

The Command window shows the following history:

```
0DEDF2E4 85C0 TE
-Read Memory data.....Succ
-Read debug register(s)....
-Read MTRR.....Succeed.
-Read MSR.....Succeed.
-Read MTRR.....Succeed.
-Read MSR.....Succeed.
```

The Source window displays the following code snippet:

```
//
// The Logging action is the critical section, so it is locked.
// The MTC assignment & update, time, and logging must be an
// atomic operation, so use the lock.
//
Status = EfiAcquireLockOrFail (&Private->DataLock);
if (EFI_ERROR (Status)) {
    //
    // Reentrancy detected so exit!
    //
    return Status;
}

Status = gBS->AllocatePool (EfiBootServicesData, TotalSize, (VOID **)&LogEntry);
if (EFI_ERROR (Status)) {
    EfiReleaseLock (&Private->DataLock);
    return EFI_OUT_OF_RESOURCES;
}
EfiZeroMem (LogEntry, TotalSize);

Record = (EFI_DATA_RECORD_HEADER *) (LogEntry + 1);
Raw = (VOID *) (Record + 1);

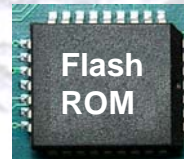
//
// Build Standard Log Header
//
Record->Version = EFI_DATA_RECORD_HEADER_VERSION;
Record->HeaderSize = sizeof (EFI_DATA_RECORD_HEADER);
```

The Local window shows the following variables:

Name	Value	Type
This	0x0D410210	*_EFI_DATA_HUB_PROTOCOL
DataRecordGuid	0x0EE52968	*EFI_GUID
ProducerName	0x0EE518A0	*EFI_GUID
DataRecordClass	0x0000000000000001	unsigned long long
RawData	0x0EE52AD0	*void
RawDataSize	0x0000007E	unsigned int
LogEntry	0x0D410210	*EFI_DATA_ENTRY
ZeroGuid	...	EFI_GUID

Patented “Virtual ROM” Technology

- No more ROM size issue: “ROM” code can be bigger than size of the flash part
- Secured implementation for “Pre-boot” environment
- No need for hidden partition
- Digitally Signed VROM image can be stored in *multiple* locations



HDD



USB Storage



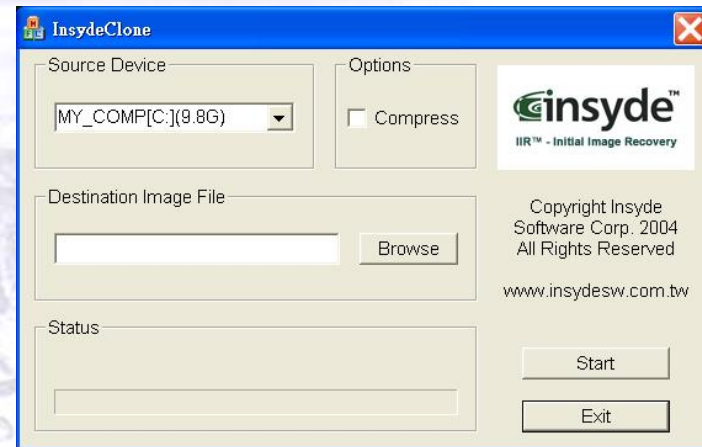
CD



Internet

Insyde IIR (Initial Image Recovery)

- VROM technology support
- Downloads and restores initial factory disk image
- UEFI based – no OS needed
- Secured application and disk image
- Recovers image from wide range of locations



Insyde UEFI Framework training programs

- “EFI Framework University” hosted by Insyde since Jan '05
- Many different levels of training. Some provided to Intel employees
- Content and materials reviewed and approved by Intel to use the logo on the certificate
- BIOS Engineers certified as “Framework Ready” at ODMs and OEMs
 - ▶ Over 250 engineers from 35 companies to date
- E-learning provides on-line training from level I to level III via Internet- over 600 audience for participate with this training now.

InsydeDIY Launched For Embedded Systems

- April 3, 2007 at Embedded Systems Conference – Silicon Valley
- Unique “Do-It-Yourself” Firmware Solution
- Royalty-free business model

*“As an Intel Communications Alliance Affiliate Member providing innovative firmware solutions, Insyde Software is an important part of our embedded ecosystem” said **Doug Davis, vice president, Digital Enterprise Group, and general manager of the Embedded Communications Group, Intel.** “With InsydeDIY, Insyde has demonstrated that they can deliver flexible and cost-effective firmware solutions that meet the needs of our embedded and communications processor customers.”*

InsydeDIY Key Benefits

- Facilitates in-house development of EFI Firmware
- Lightweight, easy to implement and cost effective
- Reduces overall project development time
- H2ODDT™ built-in software debugger
- Seamless transition path to full InsydeH2O Framework solution

Consider Insyde for UEFI Enablement

- InsydeH2O is Framework-compatible platform initialization firmware that hosts your CPU, Chipset, and boot device drivers
- InsydeH2O is modular, self-organizing, and almost all in high-level language
- InsydeH2O exposes the industry-standard UEFI Boot and Run-time interfaces used by next-gen Windows and Linux
- InsydeH2O can also boot any existing OS using CSM Legacy interface
- InsydeH2O and InsydeDIY can easily be customized to support embedded devices

Insyde Information

- Insyde web address www.insydesw.com

Insyde Software, China Office

Unit A, 4F, No.369 Jiang Su Road, Zhao
Feng World Trade Building, Shanghai P.R.C

Tel: +86 21.5240.0799

Fax: +86 21.5240.1269

Contact: Kevin Tsai

E-mail: kevin.tsai@insydesw.com.tw

Insyde Software Corp., HQ, Taiwan

6F, No. 137, Sec 2, Chien Kuo N. Rd.
Taipei, Taiwan, R. O. C.

Tel: +886.2.2506.1289

Fax: +886.2.2506.3001

E-mail: sales.tw@insydesw.com.tw