presented by

UEFI Spec Version 2.4 Facilitates Secure Update

UEFI Summerfest – July 15-19, 2013

Presented by Jeff Bobzin

Insyde Software

Agenda

- UEFI 2.4
- Background FMP
- New Capsule Defined
- Delivery on Disk
- Secure?
- Open Questions

UEFI 2.4 Spec is Public

- Some of the New Content:
  1. ARM 64-bit Bindings
  2. Custom Security Variable
  3. Variable Naming rules clarified
  4. Network driver changes including EFI_NO_MEDIA rules
  5. Async I/O Improvements
  6. Timestamp and Random Number protocols
  7. Time-based revocation
  8. Adapter Information Protocol and several AIP blocks defined
  9. Capsule Format containing FMP updates
  10. Deliver Capsule on Boot Disk
  11. Variable with Capsule processing status

UEFI 2.4 Spec is Public

- Some of the New Content:
  1. ARM 64-bit Bindings
  2. Custom Security Variable
  3. Variable Naming rules clarified
  4. Network driver changes including EFI_NO_MEDIA rules
  5. Async I/O Improvements
  6. Timestamp and Random Number protocols
  7. Time-based revocation
  8. Adapter Information Protocol and several AIP blocks defined
  9. **Capsule Format containing FMP updates**
  10. **Deliver Capsule on Boot Disk**
  11. **Variable with Capsule processing status**

Firmware Management Protocol

Background - FMP

- Added with UEFI version 2.3 update
- Designed to
  - allow individual firmware components to expose data on current running image(s)
  - accept update images

FMP in the Industry

- Mostly used in Enterprise segment
- Popular for high-performance expansion cards with multi-element firmware onboard
- But FMP is run in Boot Services – how to get the downloaded update to the FMP instance?

Factors inhibiting FMP

- Using EFI shell delivery is not secure and awkward for system admin
- For security, designers want to lock firmware store before Shell or OS boot
- Secure Boot rules block many of todays update delivery tools

UEFI 2.4 Update Has New Capsule Targeting FMP

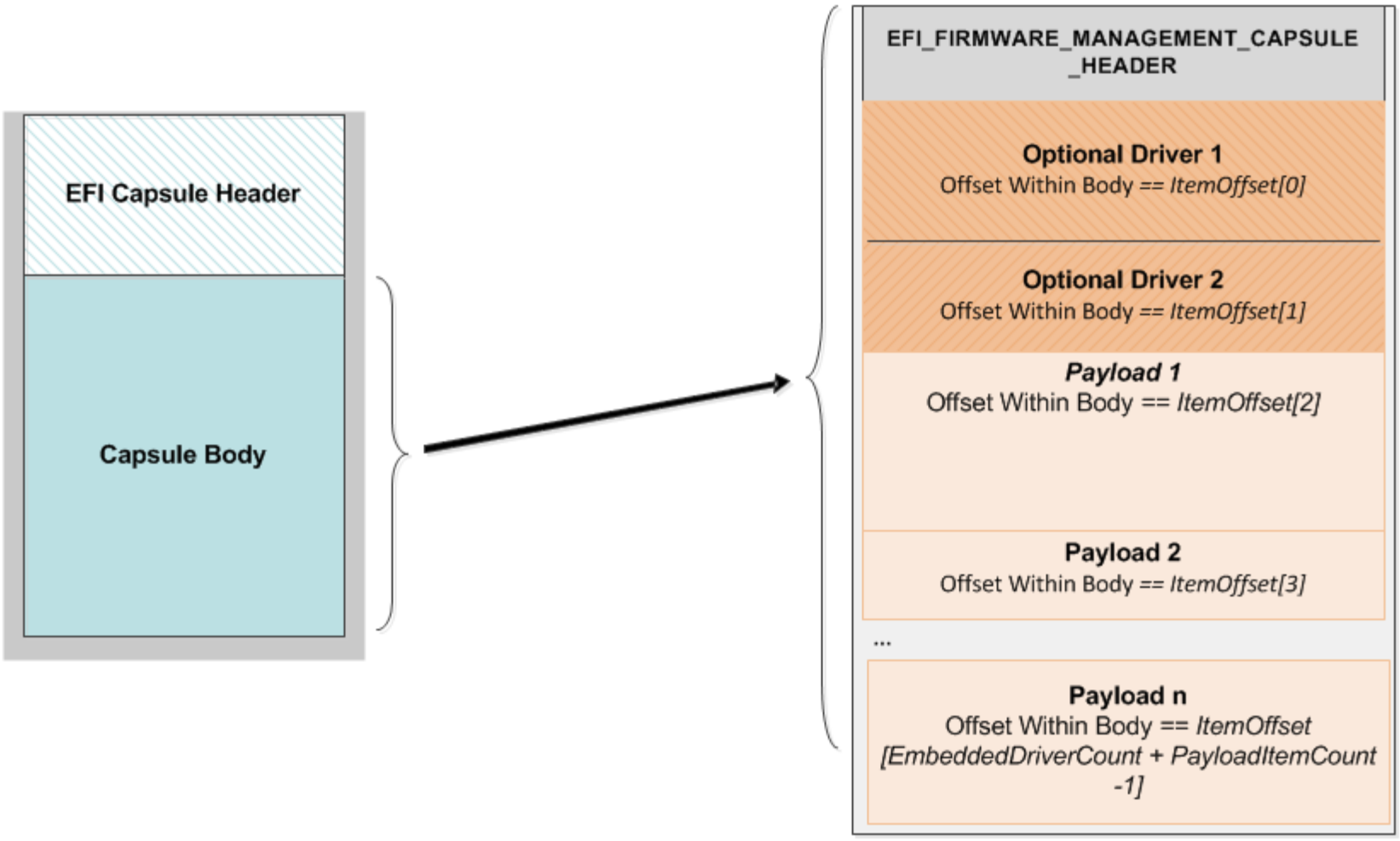
New Capsule for delivering FMP Updates

- UEFI Defines a Capsule header for UpdateCapsule() function
- UEFI 2.4 adds a complete description of internals of a Capsule targeting FMP
- System firmware unpacks the capsule and delivers updates to FMP instances early in pre-boot

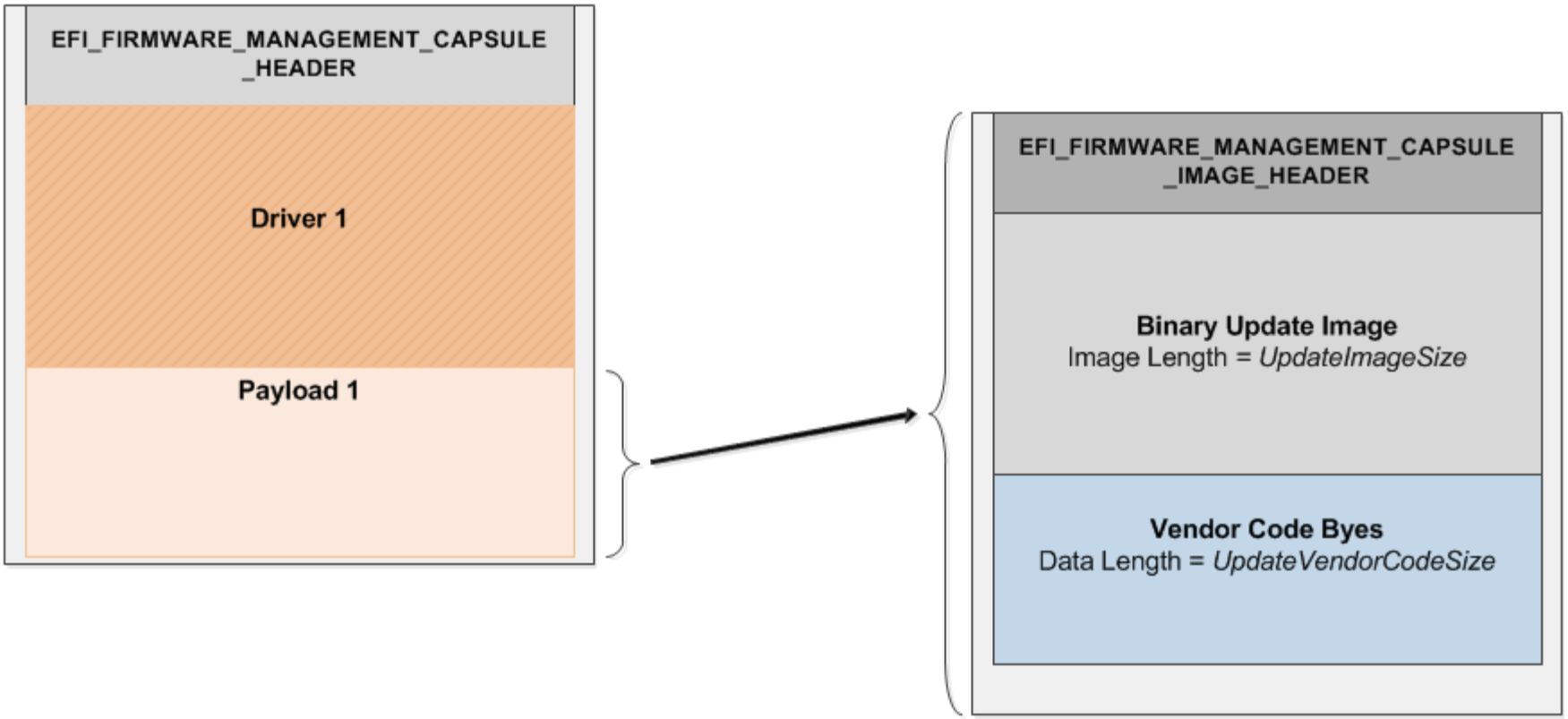
Capsule Format

- EFI_FIRMWARE_MANAGEMENT_CAPSULE_ID_GUID is the ID
- In some cases complete FMP function cannot fit inside production firmware store,
- Therefore new capsule format allows 0-n driver(s) and 0-n image(s)
- Minimum is 1 driver or 1 image

Example with 2 drivers, multiple update payloads



Payload Structure



UEFI 2.4 Update Adds New Capsule Delivery Solutions

Problem Statement

- UpdateCapsule() is run-time but:
  - FMP is not runtime so capsule needs to be conveyed to the system firmware after a restart
  - Persist in memory is possible but has disadvantages including:
    - Need to reserve block of memory of unknown size

UEFI 2.4 defines Capsule Delivery Via Disk

- OS tool Copies Capsule Image to `\EFI\CapsuleUpdate` directory on Boot Drive
- Then Sets OS_Indications bit
  - EFI_OS_INDICATIONS_FILE_CAPSULE_DELIVERY_SUPPORTED
- After Restart F/W finds Capsule and processes

UEFI 2.4 Defines Result Var

- After Capsule Processed, the result including any error status is left in created UEFI Variable
- Examined by the update launcher after OS restarts

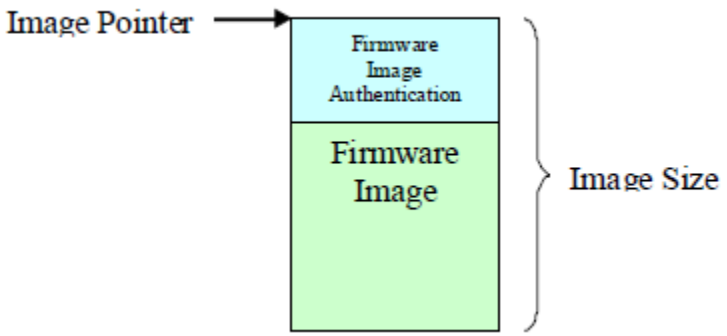
How Secure is This ‘New’ Method?

Driver Security

- Update driver launched from the capsule must be signed by CA trusted by the platform
- Same Security Level as the UEFI Option ROM (the thing that is being updated)
- The Updated Option ROM image is also checked at restart

Image Payload Security

- All FMP implementations should use IMAGE_ATTRIBUTE_AUTHENTICATION_REQUIRED



- FMP code doing check is signed, and download driver breaks any existing ROM size barrier and allows IHV to use crypto for strong image check

Discussion Questions

Non-FMP use

- I don’t use FMP for my card. Can I use this new Capsule for proprietary update?
  - Technically yes, a capsule could contain 1 or more drivers but no payloads.
  - But, the update image would need to be embedded inside the driver image and the combination sent to CA for signing…

Boot Drive Write-protected

- What about a system with a write-protected EFI System Partition?
  - Provide utility to use UpdateCapsule directly, but possible the device firmware store was locked before UpdateCapsule() caller can load?
  - What is the right event trigger for device firmware write-protect lock?

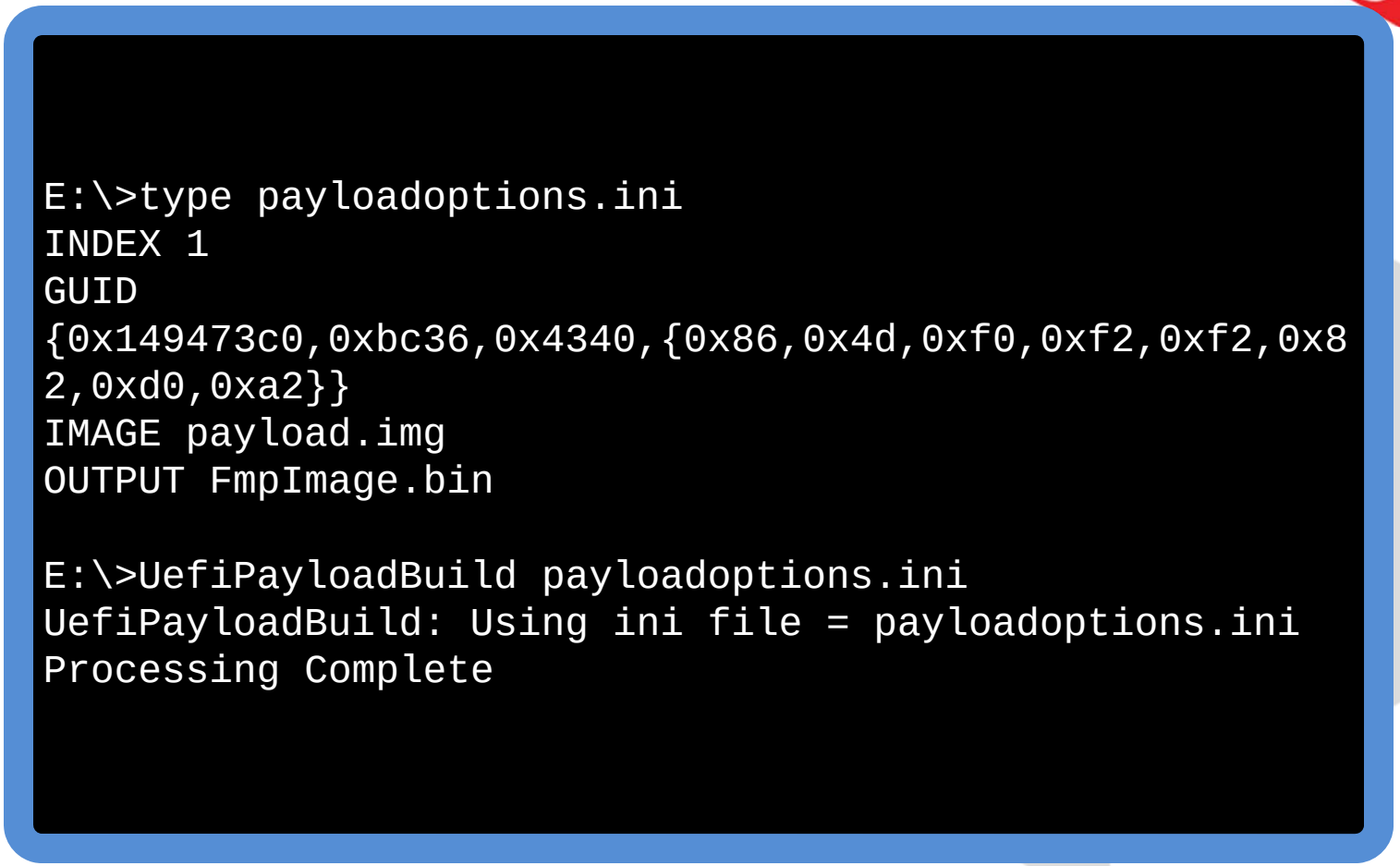
Thanks for attending the
UEFI Summerfest 2013

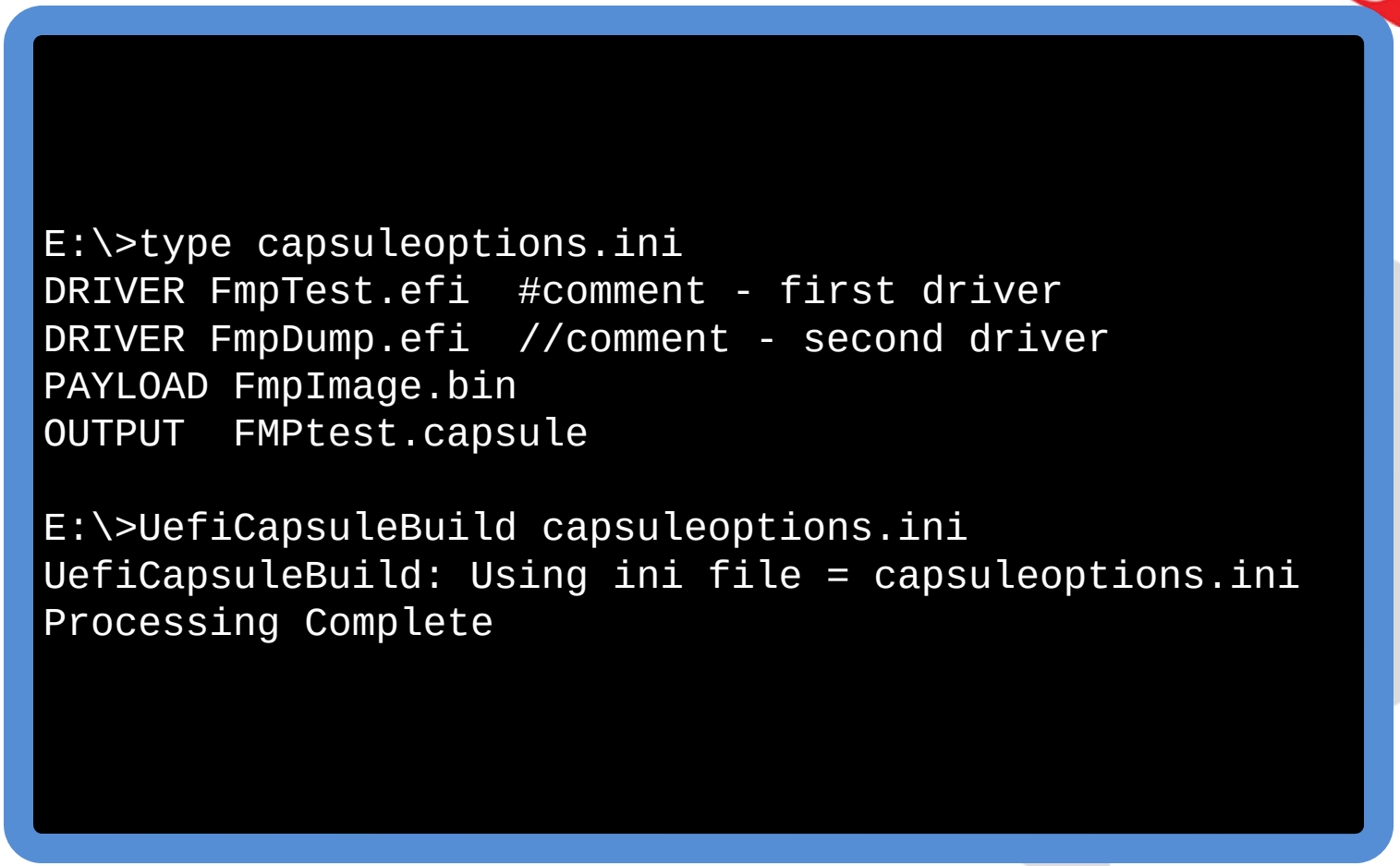
For more information on
the Unified EFI Forum and
UEFI Specifications, visit
http://www.uefi.org

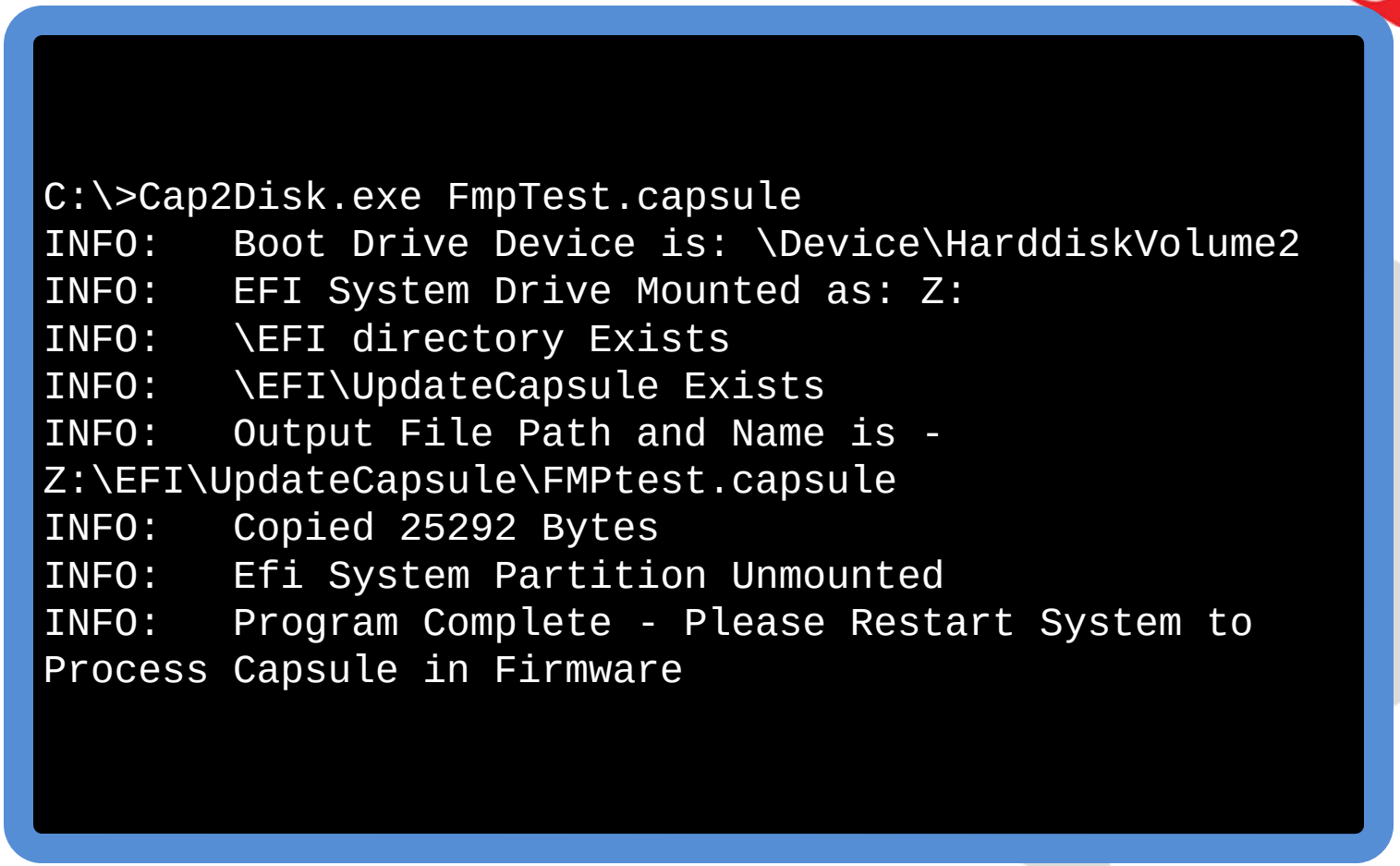
presented by

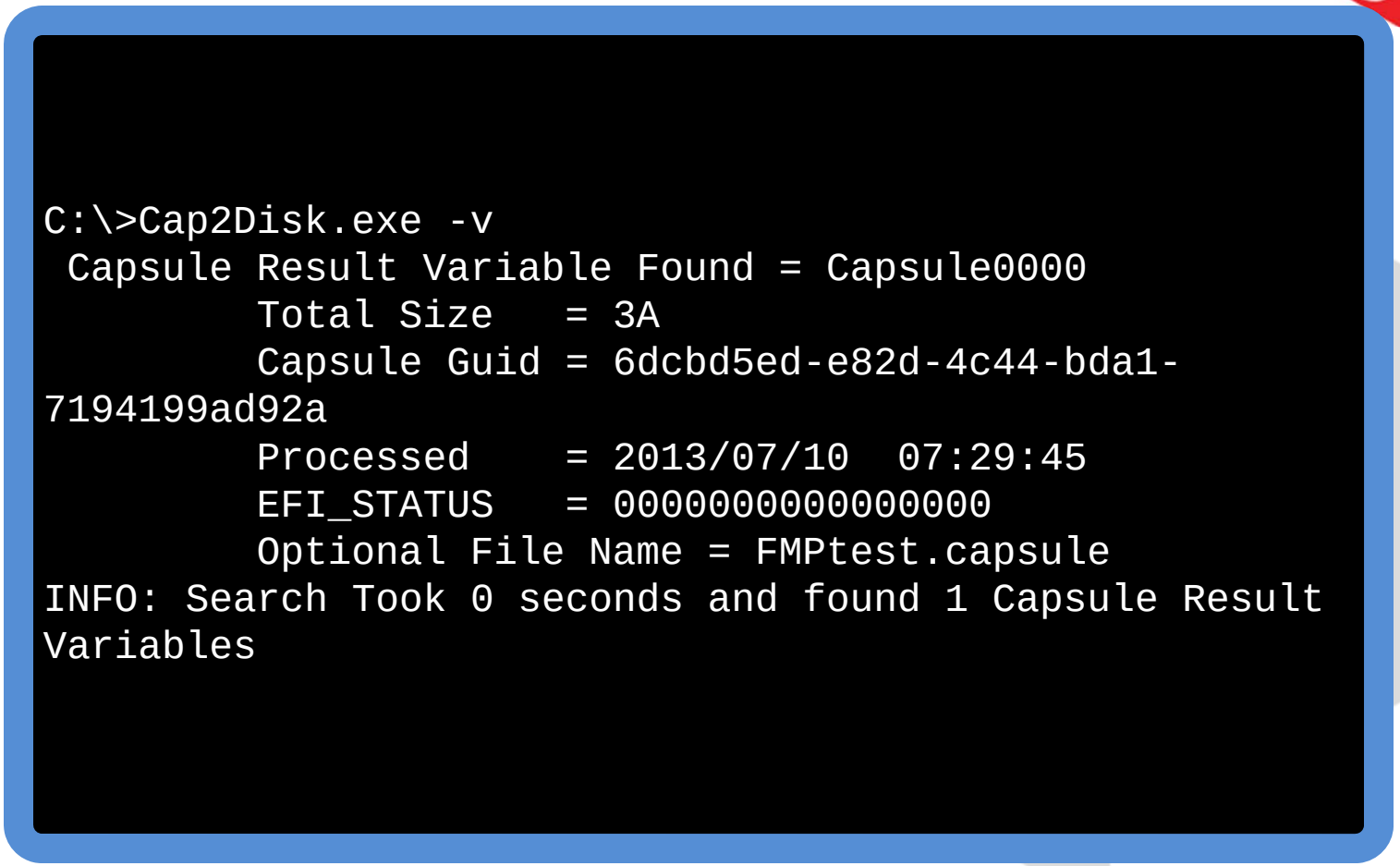
insyde®

BACKUP


E:\>type payloadoptions.ini
INDEX 1
GUID
{0x149473c0,0xbc36,0x4340,{0x86,0x4d,0xf0,0xf2,0xf2,0x8
2,0xd0,0xa2}}
IMAGE payload.img
OUTPUT FmpImage.bin
E:\>UefiPayloadBuild payloadoptions.ini
UefiPayloadBuild: Using ini file = payloadoptions.ini
Processing Complete


E:\>type capsuleoptions.ini
DRIVER FmpTest.efi #comment - first driver
DRIVER FmpDump.efi //comment - second driver
PAYLOAD FmpImage.bin
OUTPUT FMPtest.capsule
E:\>UefiCapsuleBuild capsuleoptions.ini
UefiCapsuleBuild: Using ini file = capsuleoptions.ini
Processing Complete


C:\>Cap2Disk.exe FmpTest.capsule
INFO: Boot Drive Device is: \Device\HarddiskVolume2
INFO: EFI System Drive Mounted as: Z:
INFO: \EFI directory Exists
INFO: \EFI\UpdateCapsule Exists
INFO: Output File Path and Name is -
Z:\EFI\UpdateCapsule\FMPtest.capsule
INFO: Copied 25292 Bytes
INFO: Efi System Partition Unmounted
INFO: Program Complete - Please Restart System to
Process Capsule in Firmware


C:\>Cap2Disk.exe -v
Capsule Result Variable Found = Capsule0000
Total Size = 3A
Capsule Guid = 6dcbd5ed-e82d-4c44-bda1-7194199ad92a
Processed = 2013/07/10 07:29:45
EFI_STATUS = 0000000000000000
Optional File Name = FMPtest.capsule
INFO: Search Took 0 seconds and found 1 Capsule Result Variables