Fixing Bugs in Binaries

Luis Miras

lmiras <o> gmail.com

RECON 2006

Agenda

- Introduction
- Feasibility of binary fixes
- Current third party patches
- Strategy
- Working Example
- Future of third party patches
- Questions

Introduction

- “Bah another bug !@#$%”
- Is the src available?
- What dependencies do we have?

Don't wait for a vendor to get around to it, fix vendor bugs yourself!

Feasibility of binary fixes

- Consider !/$
- Complexity of fix relative to the bug.
- Fixing an “off by one” is easy
- Adding class members can get complicated.

Current third party patches

- The most common 3rd party patches are “cracks”.
- Ilfak’s WMF patch
- Determina’s and Eeye’s CreateTextRange() patch

Strategy

Mantra : “least amount of change that gets the job done”

Strategy

1. Find the root cause of the bug
2. Locate the problem code in disassembly
3. Make a fix
4. Test, test, and test
5. Refine/Refactor the fix
6. Test, test, and test

Applying fixes

- Patching the file on disk/storage
- Patching at runtime. – injecting code, dll, hooks, etc.
- Hybrid – Loaders (packers)

Working Example

Verizon xv6700

xv6700 specs

- Windows Mobile 2005
- 416Mhz pxa270 ARM Processor
- 1.3 Mega pixel Camera
- EVDO
- WIFI
- Bluetooth
- USB ActiveSync Access

WM2005 Intro

- Part of the WinCE 5.0 family
- WinCE 5.0
- Windows Mobile 2005 Pocket PC
- Windows Mobile 2005 Smartphone
- Windows Mobile 2005 Pocket PC with Phone

WM2005 Intro

- Little Endian
- Very close to Win32
- Portable Executables
- Same style hooking
- Debugging with VS2005 and IDA ARM debugger

The Bug

- Reported on forums, pictures can’t be mailed through Gmail pop3.
- Google is performing file validation.
- JPEG corruption

Image Analysis

Virtual G – PPC imaging software

Image Analysis

- Images opened and saved from Virtual G pass the Gmail test.
- File changes only in Exif section

Image Analysis

JPEG and Exif use markers for data.

ex. FFxx

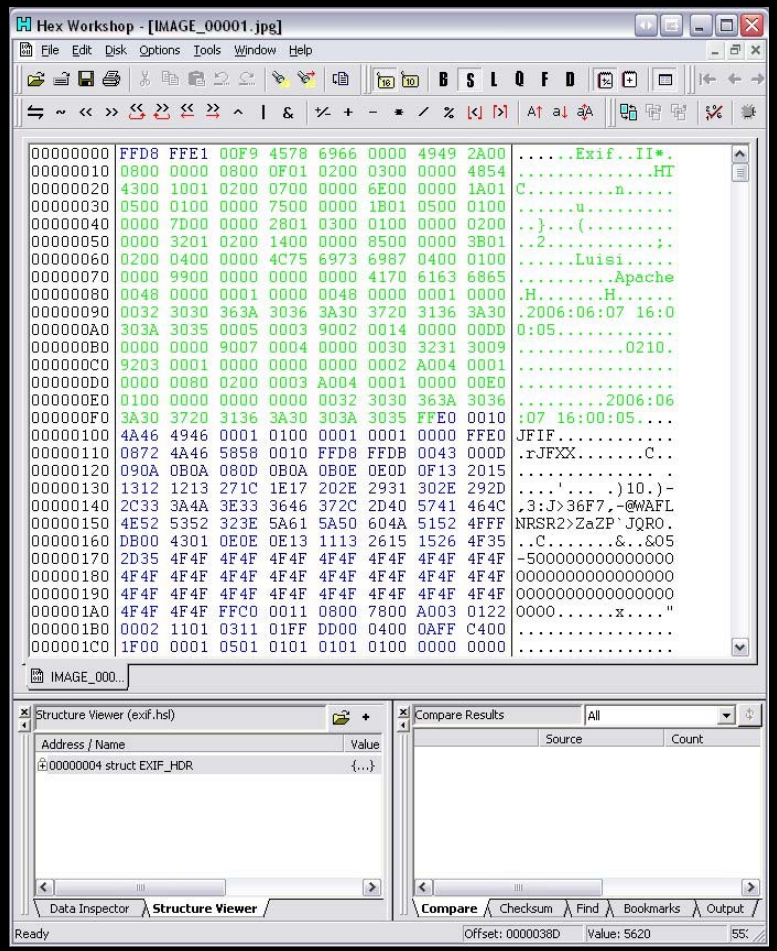
SOI Marker	APP1 Marker	APP1 Data	Other Marker
FFD8	FFE1	SSSS 457869660000 TTTT.....	FFXX SSSS DDDD.....

E1 – Start of the Exif Header

SSSS – Size field (includes 2 bytes for size field)

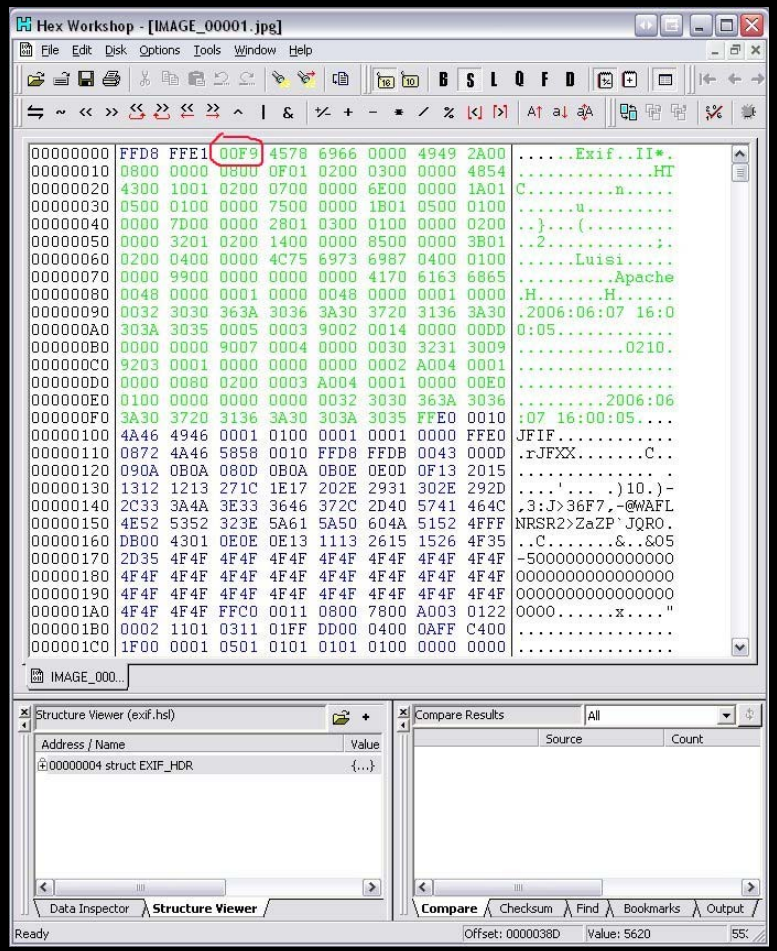
45786966 – ASCII for ‘Exif’

Image Analysis



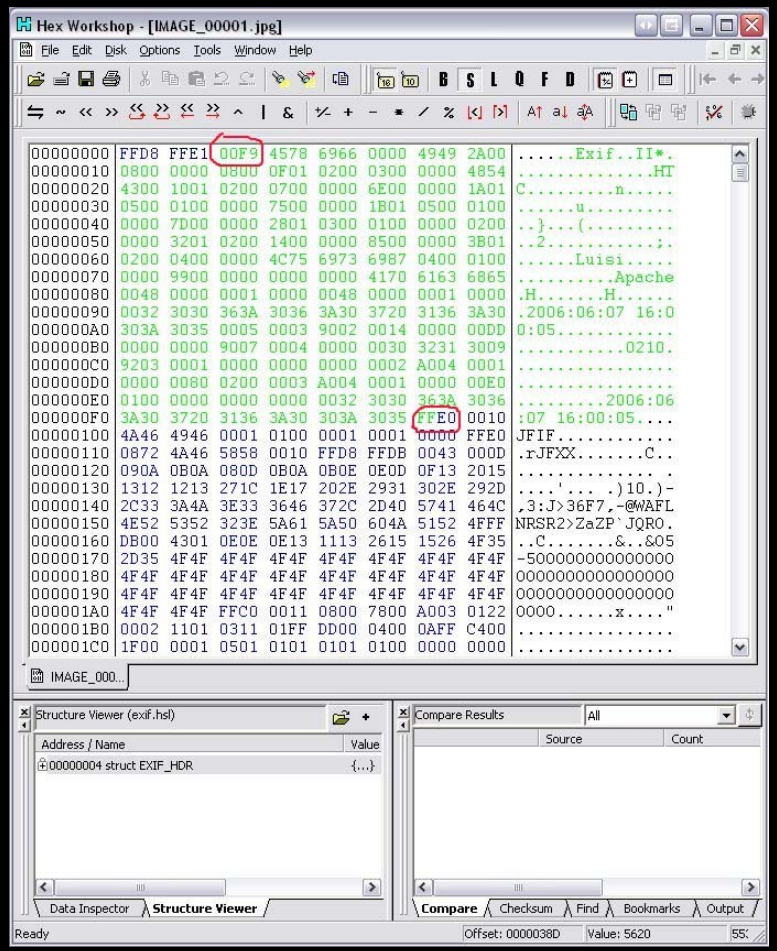
RECON 2006

Image Analysis



RECON 2006

Image Analysis



RECON 2006

Image Analysis

- Exif header is too large.
- “Off by one”

- Manually changing the size field passes the Gmail file check.
- The bug is identified!

ARM assembly intro

- RISC 32 bit
- Little/Big Endian
- 16 bit Thumb code
- Load/Store Architecture

http://blogs.msdn.com/windowsmobile/archive/2005/05/10/ArmTutorial.aspx

Registers

16 Registers

R0-R3 General, functions args

R4-R11, R12 General

SP Stack Pointer

PC Program Counter

LR Link Register

Instructions

Assembly mostly reads right to left like Intel

```
mov reg, reg
mov reg, #0x00

ldrb reg, address

strb reg, address
```

Camera.exe Analysis

- Copy it to PC using ActiveSync connection
- IDA identifies file as an ARM PE
- Flirt recognizes WinCE libs

Bug in Disassembly

- Need to locate the bug in disassembly
- Locate construction of Exif header
- “Exif” not found in strings list

Bug in Disassembly

- Look for individual letters being written out.

```
mov register, #0x45 ; ‘E’
strb register, buffer
```

...

Success at function 0x05BCC0

Bug in Disassembly

```
0005BD38   MOV    R1, #0x45      ; E
0005BD3C   STRB    R1, [R2,#2]
[ snip ]
0005BD58   MOV    R0, #0x78      ; x
0005BD5C   STRB    R0, [R2]
[ snip ]
0005BD78   MOV    R0, #0x69      ; i
0005BD7C   STRB    R0, [R2]
[ snip ]
0005BD98   MOV    R0, #0x66      ; f
0005BD9C   STRB    R0, [R2]
```

Runtime Analysis

- Combining runtime and static analysis speeds up the process
- Visual Studio 2005 debugger can connect to devices over ActiveSync

http://www.airscanner.com/security/WM5debugVS2005.pdf

Runtime Analysis

- Set break points on function `0x05BCC0` and xref function(parent)
- ‘E’ gets written to a buffer identifying the location of size
- “Watch” for the size being written

Runtime Analysis

Size writing identified:

```
05BF7C  ADD     R0, R3, #0xFF00
05BF80  ADD     R1, R0, #0xFE
05BF84  MOV     R2, R1,LSL#16
05BF88  MOV     R0, R2,LSR#16
05BF8C  MOV     R1, R0,LSR#8
05BF90  ADD     R0, R3, #0xFE
05BF94  STRB    R1, [R4]     ; size write
05BF98  AND     R2, R1, #0xFF
05BF9C  STRB    R0, [R4,#1] ; size write
```

Fix

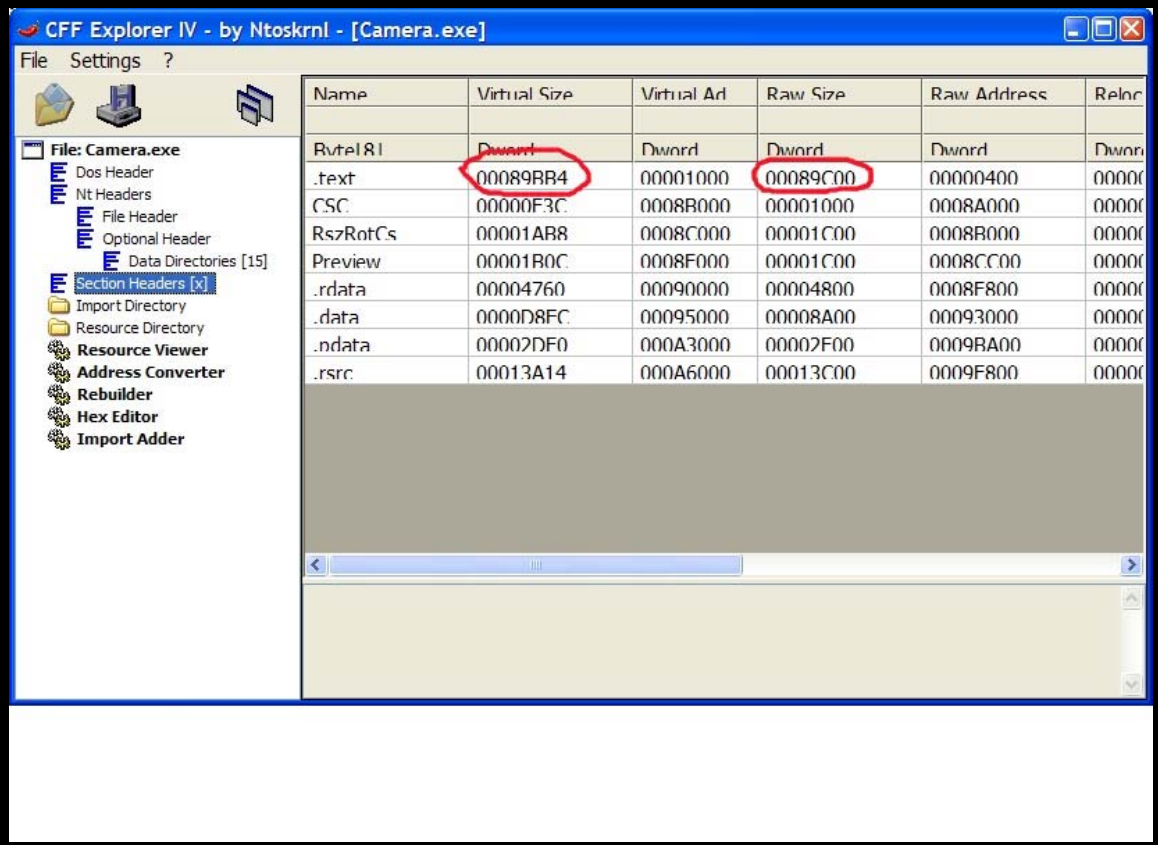
The fix can divert execution before the last write (lsb).

A branch is put in, but first space to put in code must be found.

Where to patch?

- Code caves between functions
- Extending sections
- New sections

Extending a Section



RECON 2006

Extending a Section

.text section virtual size = 0x89BB4

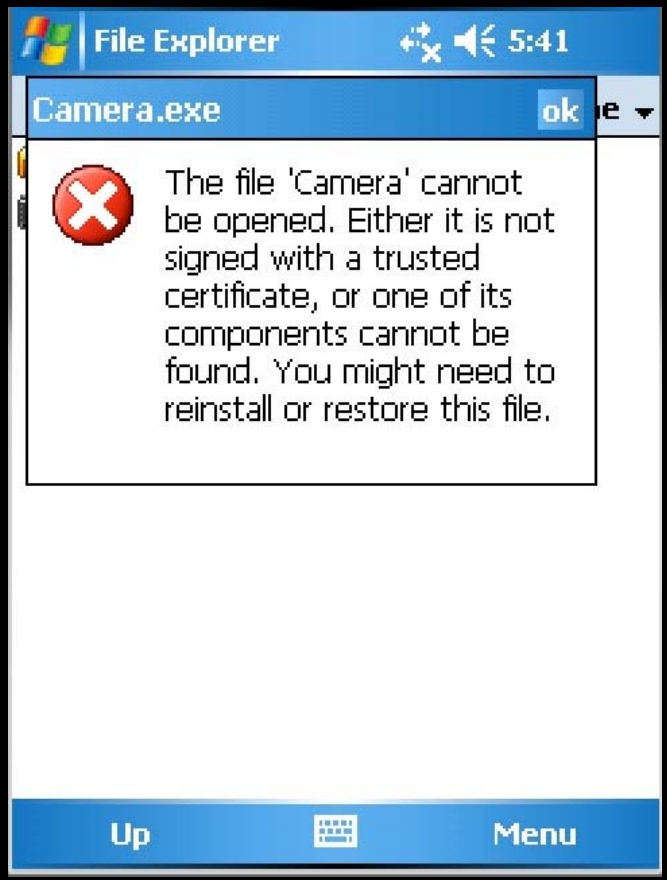
.text section raw size = 0x89C00

Virtual size can be increased to 0x89C00
Producing 0x4C of extra space

The Fix

```
05BF9C  STRB  R0, [R4,#1]          B  loc_9ABC0
05BFA0  AND   R1, R0, #0xFF        MOV  R9, R9
05BFA4  ADD   R0, SP, #0x10+arg_4  MOV  R9, R9
05BFA8  BL    sub_48400            MOV  R9, R9
05BFAC  MOV   R0, #1               MOV  R9, R9
05BFB0  LDMFD SP, {R4,R5,SP,PC}    MOV  R9, R9
-----------------------------------------------
09ABC0  SUB     R11, R0, #1
09ABC4  STRB    R11, [R4,#1]
09ABC8  AND     R1, R0, #0xFF
09ABCC  ADD     R0, SP, #0x10+arg_4
09ABD0  BL      sub_48400
09ABD4  MOV     R0, #1
09ABD8  LDMFD   SP, {R4,R5,SP,PC}
```

Signed Code Error



RECON 2006

Signed Code Fix

Signed code is pointed to by the Security Data Directory in the PE header.

Set RVA and size to NULL.

Signed Code Fix

CFF Explorer IV - by Ntoskrnl - [Camera.exe]

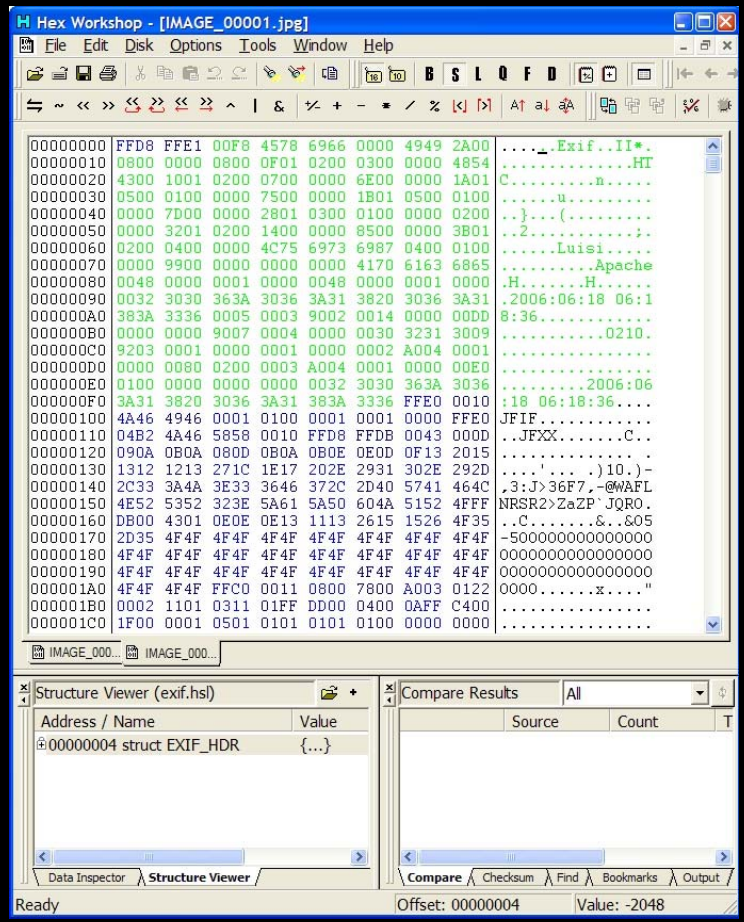
File Settings ?

- File: Camera.exe
  - Dos Header
  - Nt Headers
    - File Header
    - Optional Header
      - Data Directories [15]
  - Section Headers [x]
  - Import Directory
  - Resource Directory
  - **Resource Viewer**
  - **Address Converter**
  - **Rebuilder**
  - **Hex Editor**
  - **Import Adder**

Member	Offset	Size	Value
Export Directory RVA	00000180	Dword	00000000
Export Directory Size	00000184	Dword	00000000
Import Directory RVA	00000188	Dword	00093628
Import Directory Size	0000018C	Dword	00000168
Resource Directory RVA	00000190	Dword	000A6000
Resource Directory Size	00000194	Dword	00013A14
Exception Directory RVA	00000198	Dword	000A3000
Exception Directory Size	0000019C	Dword	00002DF0
Security Directory RVA	000001A0	Dword	000B2400
Security Directory Size	000001A4	Dword	00000370
Relocation Directory RVA	000001A8	Dword	00000000
Relocation Directory Size	000001AC	Dword	00000000
Debug Directory RVA	000001B0	Dword	00090000
Debug Directory Size	000001B4	Dword	0000001C
Architecture Directory RVA	000001B8	Dword	00000000
Architecture Directory Size	000001BC	Dword	00000000
Reserved	000001C0	Dword	00000000
Reserved	000001C4	Dword	00000000
TLS Directory RVA	000001C8	Dword	00000000
TLS Directory Size	000001CC	Dword	00000000
Configuration Directory	000001D0	Dword	00000000

RECON 2006

Results



RECON 2006

Bug in the Fix

The fix contains a bug if the size is:
0xXX00

For example:
0x0100 becomes 0x01FF

A Better Fix

A better fix can be done without extending a section.

Changing only 2 bytes

A Better Fix

```
05BF80   ADD     R1, R0, #0xFE ; 0xFD
05BF84   MOV     R2, R1,LSL#16
05BF88   MOV     R0, R2,LSR#16
05BF8C   MOV     R1, R0,LSR#8
05BF90   ADD     R0, R3, #0xFE ; 0xFD
05BF94   STRB    R1, [R4]
05BF98   AND     R2, R1, #0xFF
05BF9C   STRB    R0, [R4,#1]
```

A Better Fix

On the file patch:

Offset 0x4B380: 0xFE -> 0xFD

Offset 0x4B390: 0xFE -> 0xFD

Bonus Patch

Exif header contains various fields:

Date/time

Camera Vendor

Camera Model

Artist Name aka your name in every image

Bonus Patch

- Artist name comes from the Owner name stored on the phone.
- Camera.exe accesses name through the registry.
- From IDA string list: “ControlPanel\Owner\Owner”

Bonus Patch

Within the disassembly:

```
000481AC LDR R0, =aControlpanelOw
000481B0 MOV R3, #0x80000001
000481B4 MOV R2, #0x280
000481B8 MOV R1, R5
000481BC BL get_reg_key2
000481C0 CMP R0, #0
000481C4 BEQ done_with_regkeys
```

Bonus Patch

get_reg_keys2 – returns registry value or Null if not found

Change:

```
000481C0  00 00 50 E3   CMP R0, #0
```

To

```
000481C0  00 00 50 E1   CMP R0, R0; always equal

000481C4 BEQ done_with_regkeys
```

Bonus Patch

On the file patch:

Offset 0x0375C3: 0xE3 -> 0xE1

Bonus Patch

Hex Workshop - [IMAGE_00002.jpg]

File Edit Disk Options Tools Window Help

00000000	FFD8	FFE1	00EC	4578	6966	0000	4949	2A00	....ᵢ.Exif..II*.
00000010	0800	0000	0700	0F01	0200	0300	0000	4854	..............HT
00000020	4300	1001	0200	0700	0000	6200	0000	1A01	C.........b.....
00000030	0500	0100	0000	6900	0000	1B01	0500	0100	......i.........
00000040	0000	7100	0000	2801	0300	0100	0000	0200	..q...(.........
00000050	0000	3201	0200	1400	0000	7900	0000	6987	..2.......y...i.
00000060	0400	0100	0000	8D00	0000	0000	0000	4170	..............Ap
00000070	6163	6865	0048	0000	0001	0000	0048	0000	ache.H.......H..
00000080	0001	0000	0032	3030	363A	3036	3A31	3820	.....2006:06:18
00000090	3036	3A32	313A	3437	0005	0003	9002	0014	06:21:47........
000000A0	0000	00D1	0000	0000	9007	0004	0000	0030	0
000000B0	3231	3009	9203	0001	0000	0000	0000	0002	210.............
000000C0	A004	0001	0000	0080	0200	0003	A004	0001	....
000000D0	0000	00E0	0100	0000	0000	0000	0032	3030	200
000000E0	363A	3036	3A31	3820	3036	3A32	313A	3437	6:06:18 06:21:47
000000F0	FFE0	0010	4A46	4946	0001	0100	0001	0001	....JFIF........
00000100	0000	FFE0	04B6	4A46	5858	0010	FFD8	FFDB	......JFXX......
00000110	0043	000D	090A	0B0A	080D	0B0A	0B0E	0E0D	.C..............
00000120	0F13	2015	1312	1213	271C	1E17	202E	2931	.. ..'... .)1
00000130	302E	292D	2C33	3A4A	3E33	3646	372C	2D40	0.)-,3:J>36F7,-@
00000140	5741	464C	4E52	5352	323E	5A61	5A50	604A	WAFLNRSR2>ZaZP`J
00000150	5152	4FFF	DB00	4301	0E0E	0E13	1113	2615	QRO...C.......&.
00000160	1526	4F35	2D35	4F4F	4F4F	4F4F	4F4F	4F4F	.&O5-5OOOOOOOOOO
00000170	4F4F	4F4F	4F4F	4F4F	4F4F	4F4F	4F4F	4F4F	OOOOOOOOOOOOOOOO
00000180	4F4F	4F4F	4F4F	4F4F	4F4F	4F4F	4F4F	4F4F	OOOOOOOOOOOOOOOO
00000190	4F4F	4F4F	4F4F	4F4F	FFC0	0011	0800	7800	OOOOOOOO......x.
000001A0	A003	0122	0002	1101	0311	01FF	DD00	0400	..."............
000001B0	0AFF	C400	1F00	0001	0501	0101	0101	0100	....
000001C0	0000	0000	0000	0001	0203	0405	0607	0809	....

IMAGE_000...

Structure Viewer (exif.hsl)

Address / Name	Value
00000004 struct EXIF_HDR	{...}

Data Inspector | Structure Viewer

Compare Results — All

	Source	Count	T

Compare | Checksum | Find | Bookmarks | Output

Ready | Offset: 00000004 | Value: -5120

RECON 2006

Future of 3rd party patches

- Continued release of 3rd party security patches
- Advisories released with binary fix diffs
- Vulnerability market consisting of both 0day exploit and 0day patches

Questions ?

RECON 2006

Shameless Self-Promotion

Automating Exploit Detection: Cutting-edge Tools and Techniques
Matt Hargett & Luis Miras
Blackhat Training USA

Bridging the Gap between Static & Dynamic Reversing
Defcon 14

RECON 2006