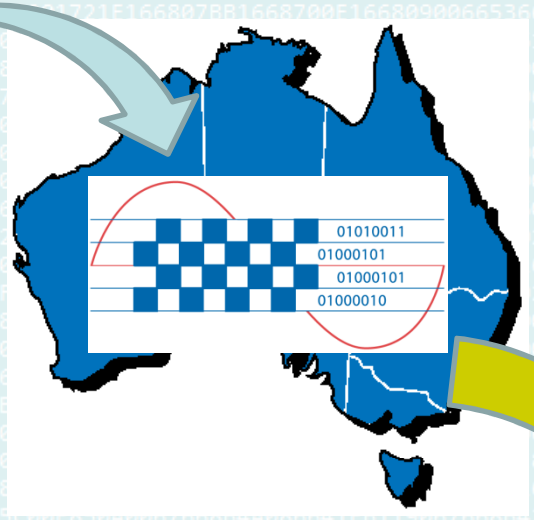
CHAMPLAIN COLLEGE

NTFS bit by byte

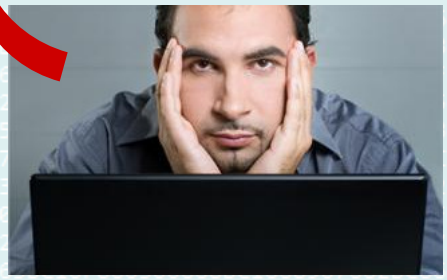
By: Mike Wilkinson

CHAMPLAIN COLLEGE

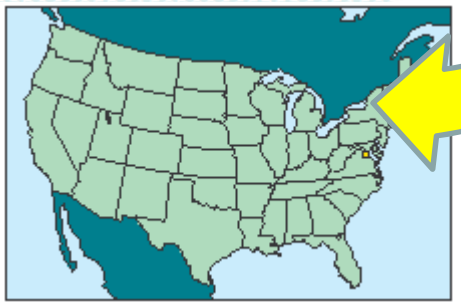
About Mike



ACU
AUSTRALIAN CATHOLIC UNIVERSITY



IT Contractor



CHAMPLAIN COLLEGE
BURLINGTON, VERMONT

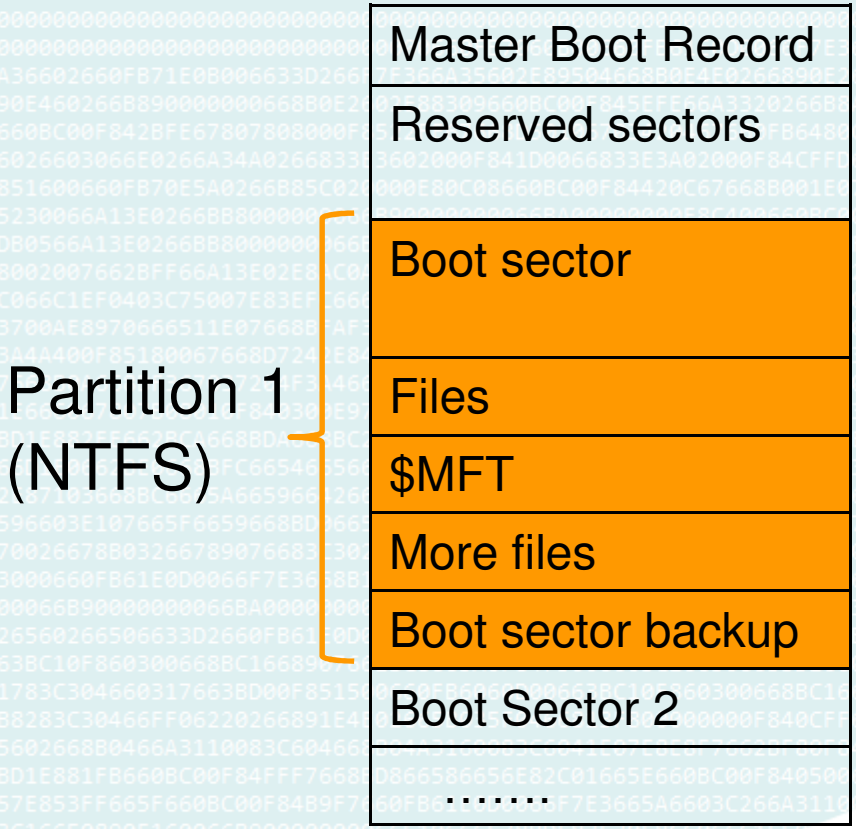
CHAMPLAIN COLLEGE

Disclaimer

- Information from multiple sources:
  - Microsoft (authoritative?)
  - Carrier (2005) *File system Forensic Analysis*
  - Other training courses
  - Online (e.g. ntfs.com)
  - Experimentation & testing
- Problem, there are differences!
- MS terminology is used where known

CHAMPLAIN COLLEGE

Disk layout



CHAMPLAIN COLLEGE

Everything is a file

- Boot sector contain BPB
- BPB points to $MFT & $MFTMirr
- $MFT points to boot sector ($boot)….

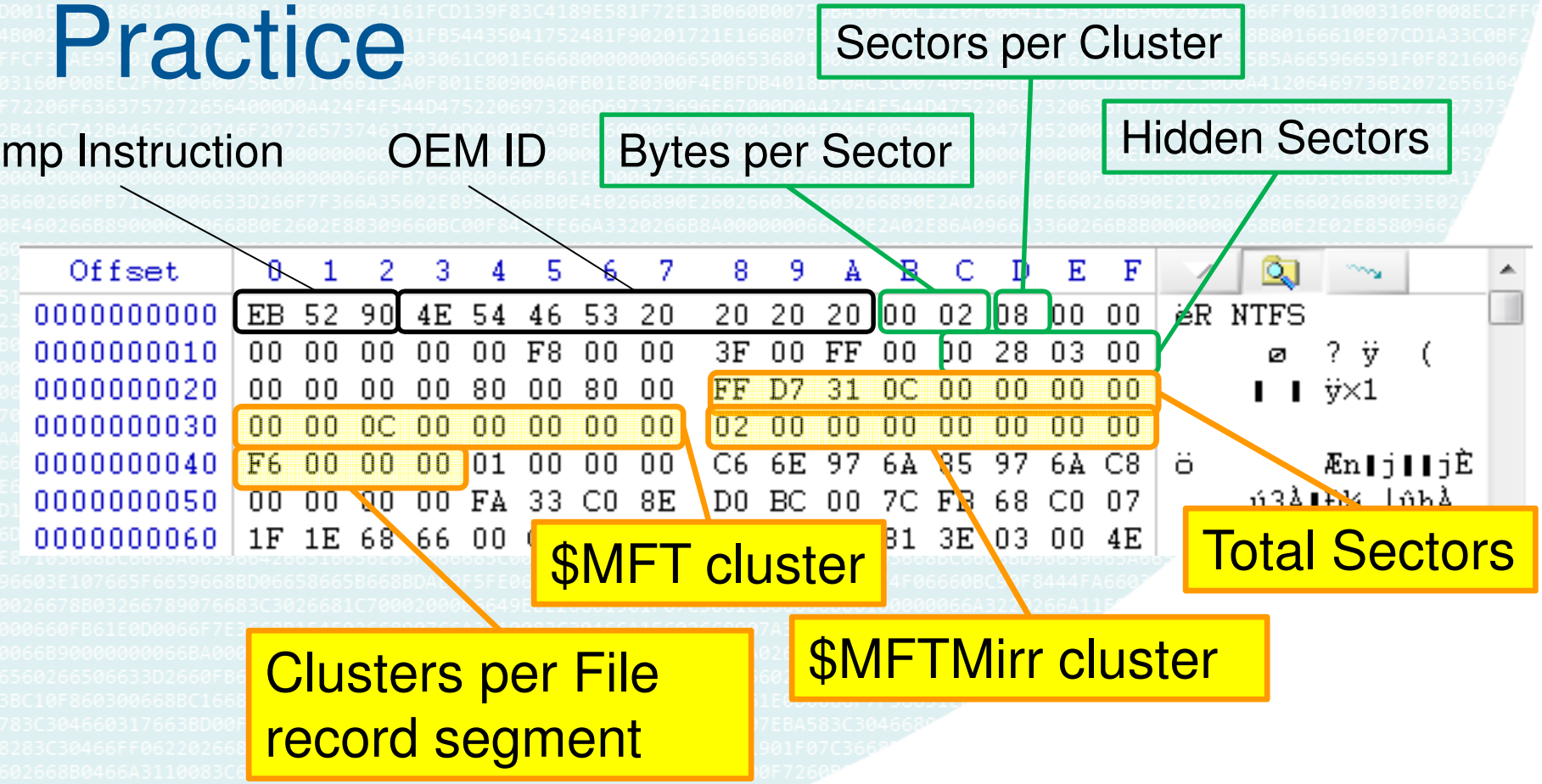
CHAMPLAIN COLLEGE

Boot Sector

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Jump Instruction			OEM ID								Bytes/ Sector		Sect/ clust	res	
10	0x000000			unused		Media desc	0x0000		Sect / track		Number heads	Hidden Sectors				
20	unused								Total Sectors							
30	Logical Cluster of $MFT								Logical Cluster of $MFTMirr							
40	Clust / File record segment			Clusters / Index Block					Volume Serial Number							
50	Checksum			Boot Code												
60	Boot Code															
...																
1E0																
1F0	Boot Code													55	AA	

CHAMPLAIN COLLEGE

Practice



CHAMPLAIN COLLEGE

BUT

- Intel processor reads number right to left
- 

= 0x0200 = 512
- Boot sector is at cluster 0

CHAMPLAIN COLLEGE

Practice…

Jump Instruction

OEM ID

Bytes per Sector
0x0200
512

Sectors per Cluster
8

Hidden Sectors
0x032800
206,848

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
0000000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	28	03	00
0000000020	00	00	00	00	80	00	80	00	FF	D7	31	0C	00	00	00	00
0000000030	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00
0000000040	F6	00	00	00	01	00	00	00	C6	6E	97	6A	85	97	6A	C8
0000000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
0000000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00

Clusters per File record segment
0xF6 = 246

$MFT cluster
0x0C0000 = 786432

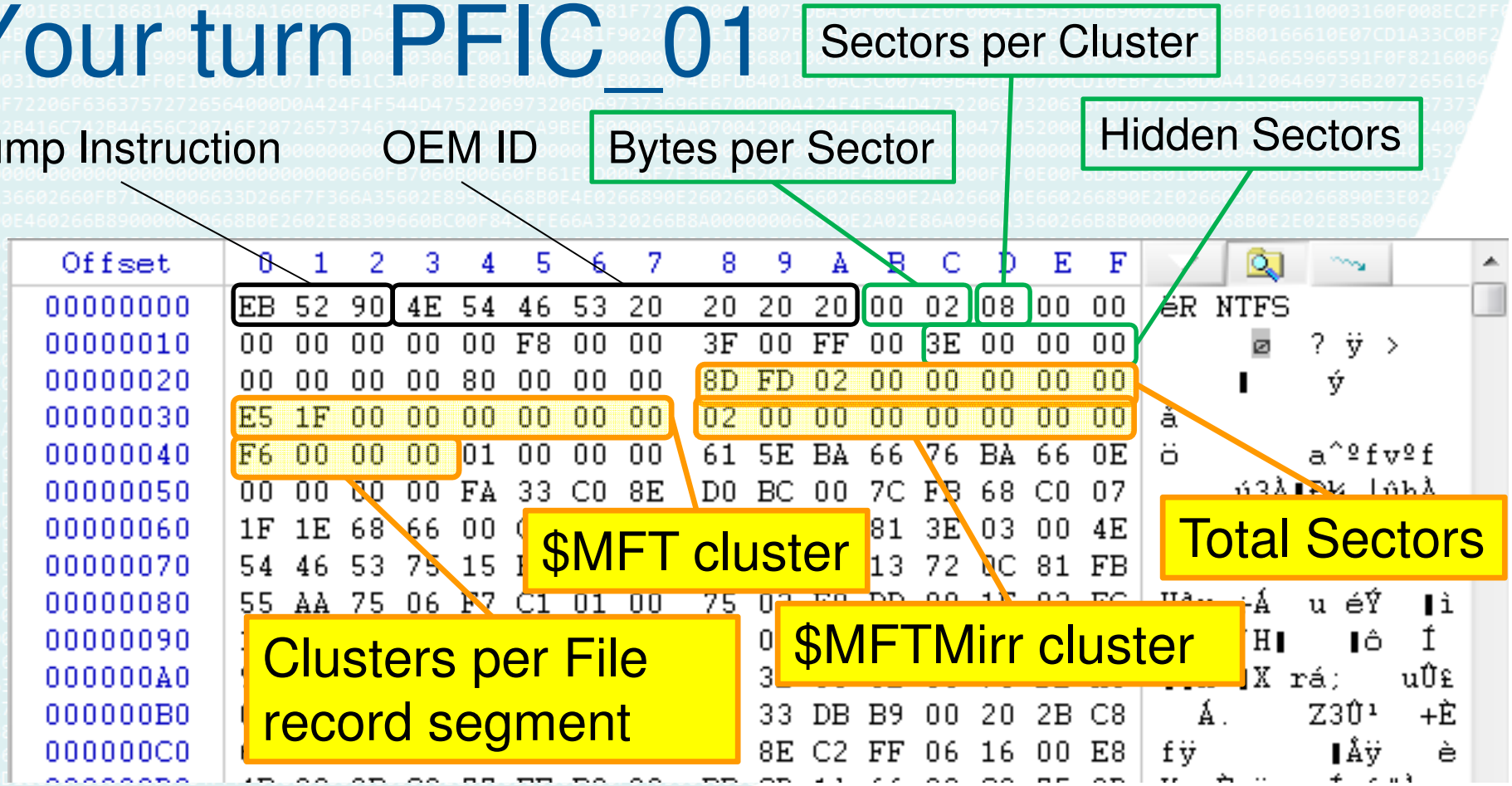
$MFTMirr cluster
0x02

Total Sectors
0x0C31D7FF =
204,593,151

97GiB

CHAMPLAIN COLLEGE

Your turn PFIC_01



CHAMPLAIN COLLEGE

Your turn…

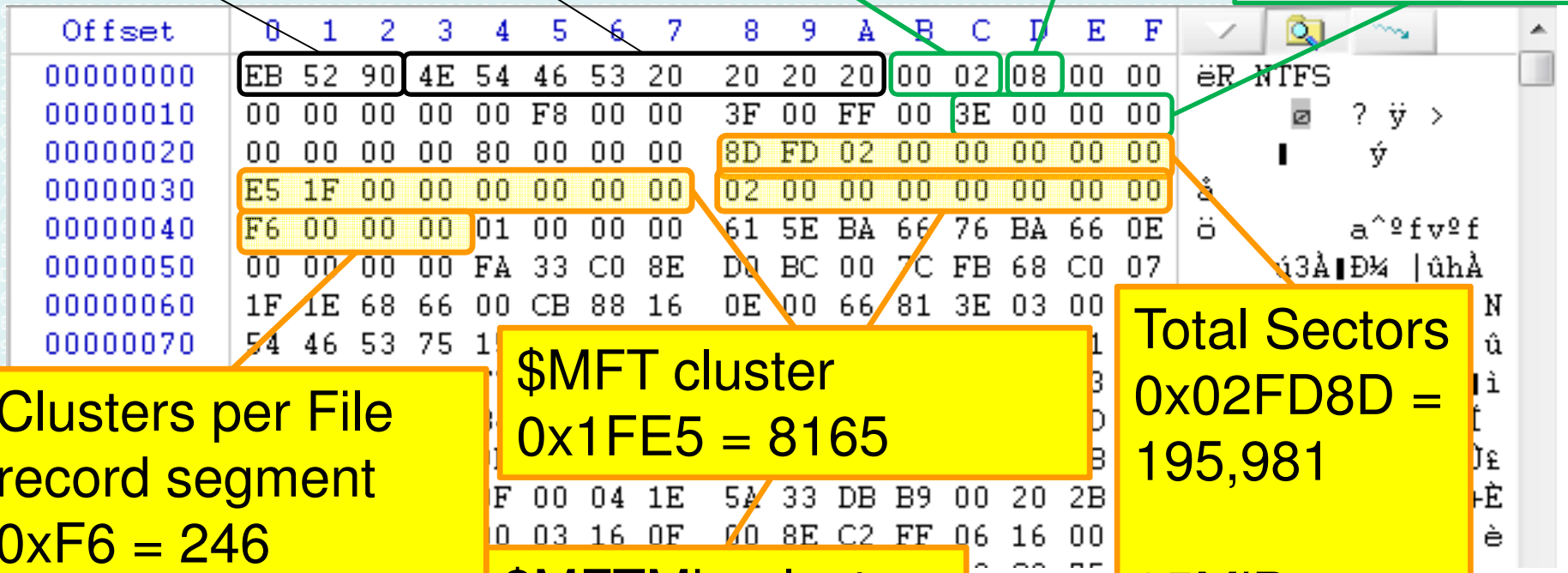
Jump Instruction

OEM ID

Bytes per Sector
0x0200
512

Sectors per Cluster
8

Hidden Sectors
0x0000003E
62



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	3E	00	00	00
00000020	00	00	00	00	80	00	00	00	8D	FD	02	00	00	00	00	00
00000030	E5	1F	00	00	00	00	00	00	02	00	00	00	00	00	00	00
00000040	F6	00	00	00	01	00	00	00	61	5E	BA	66	76	BA	66	0E
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
00000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	
00000070	54	46	53	75	1											

Clusters per File record segment
0xF6 = 246

$MFT cluster
0x1FE5 = 8165

$MFTMirr cluster
0x02

Total Sectors
0x02FD8D = 195,981

95MiB

CHAMPLAIN COLLEGE

Where is the $MFT?

- Cluster 786,432
- 1 sector = 512 bytes
- 1 cluster = 8 sectors
- $MFT starts at byte 786,432 x 512 x 8
  = 3,221,225,472
  =0xC0000000

CHAMPLAIN COLLEGE

Your turn 2 – Find the $MFT on PFIC_01

- $MFT start cluster =
- 1 sector = ??? bytes
- 1 cluster = ? sectors
- $MFT starts at byte x x
  =

CHAMPLAIN COLLEGE

Where is the $MFT on PFIC_01?

$MFT start cluster = 0x1FE5 = 8165

1 sector = 512 bytes

1 cluster = 8 sectors

$MFT starts at byte 8165 x 512 x 8

= 33,443,840

= 0x1FE5000

CHAMPLAIN COLLEGE

NTFS files…

Everything is a file

File	Name	record #
$MFT	Master File Table	0
$MFTMirr	MFT mirror	1
$LogFile	Log file	2
$Volume	Volume	3
$AttrDef	Attribute definitions	4
.	Root file name index	5
$Bitmap	Cluster bitmap	6
$Boot	Boot sector	7
$BadClus	Bad cluster file	8
$Secure	Security File	9
$Upcase	Upcase table	10
$Extend	NTFS extension file	11
	reserved	12-15

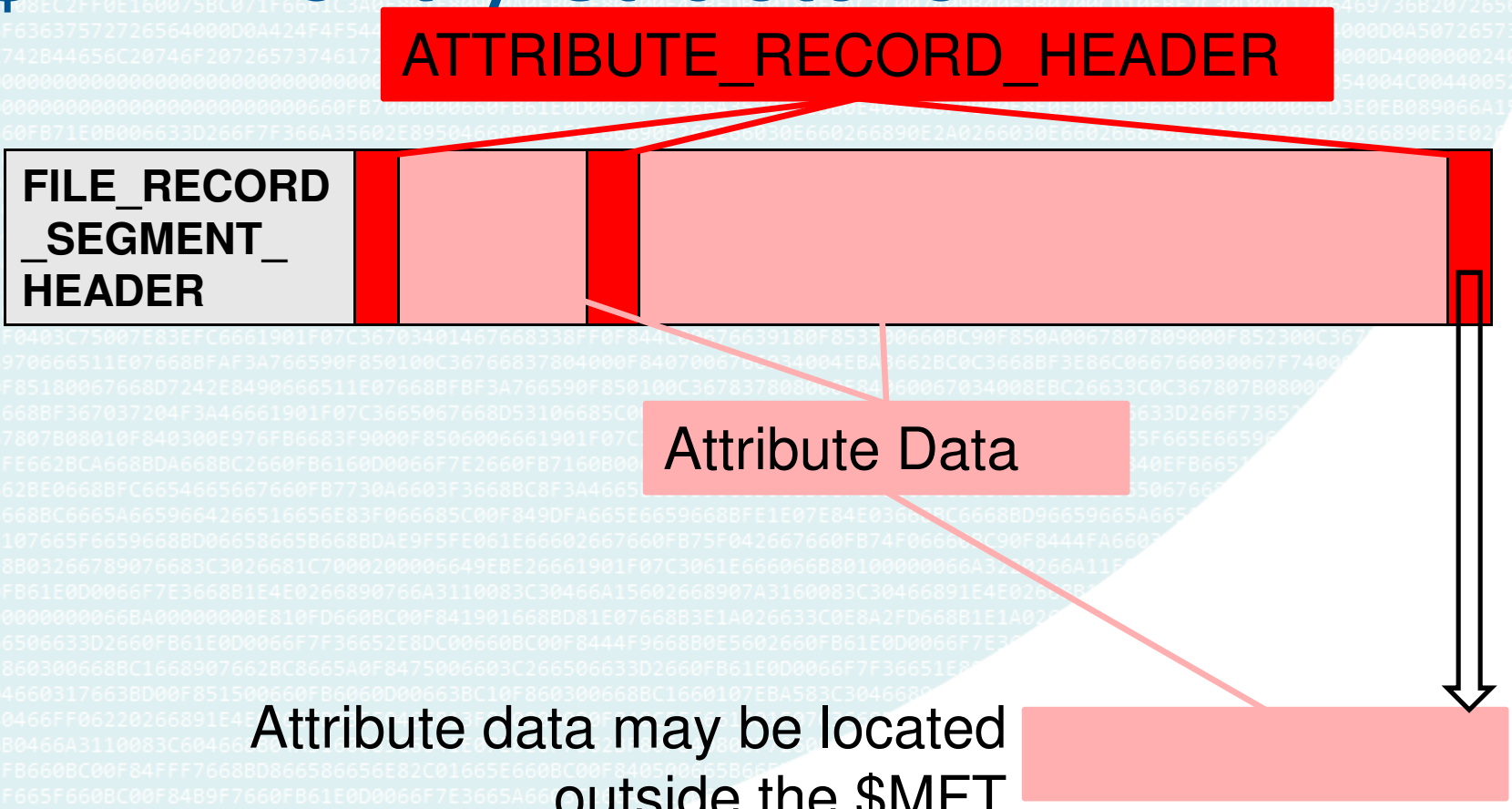
CHAMPLAIN COLLEGE

$MFT

- Contains a record for every file
- Each record is a chain of attributes
- Default record size 1024 bytes
- May contain empty records
- Default size determined by partition size

CHAMPLAIN COLLEGE

$MFT entry structure



CHAMPLAIN COLLEGE

FILE_RECORD_SEGMENT_HEADER

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F	I	L	E	Update Seq array offset		Update Seq array size		$LogFile Sequence Number							
1	Seq no		Hard Link Count		1st attrib offset		Flags		Used size of file record				Allocated size of file record			
2	File reference to base file record								Next attrib ID				MFT Record No			
3	default location of update seq array (size determined by seq size)						Reserved for update sequence array?									
	Reserved for sequence array?								Common location of 1st attrib							

CHAMPLAIN COLLEGE

FILE_RECORD_SEGMENT_HEADER

- Update sequence – integrity checking if record during move or copy
- $LogFile seq num – Reference to entry in $LogFile (journal)
- Sequence num – number of times record has been updated
- Flags – 0x0001 = in use
  0x0002 = directory

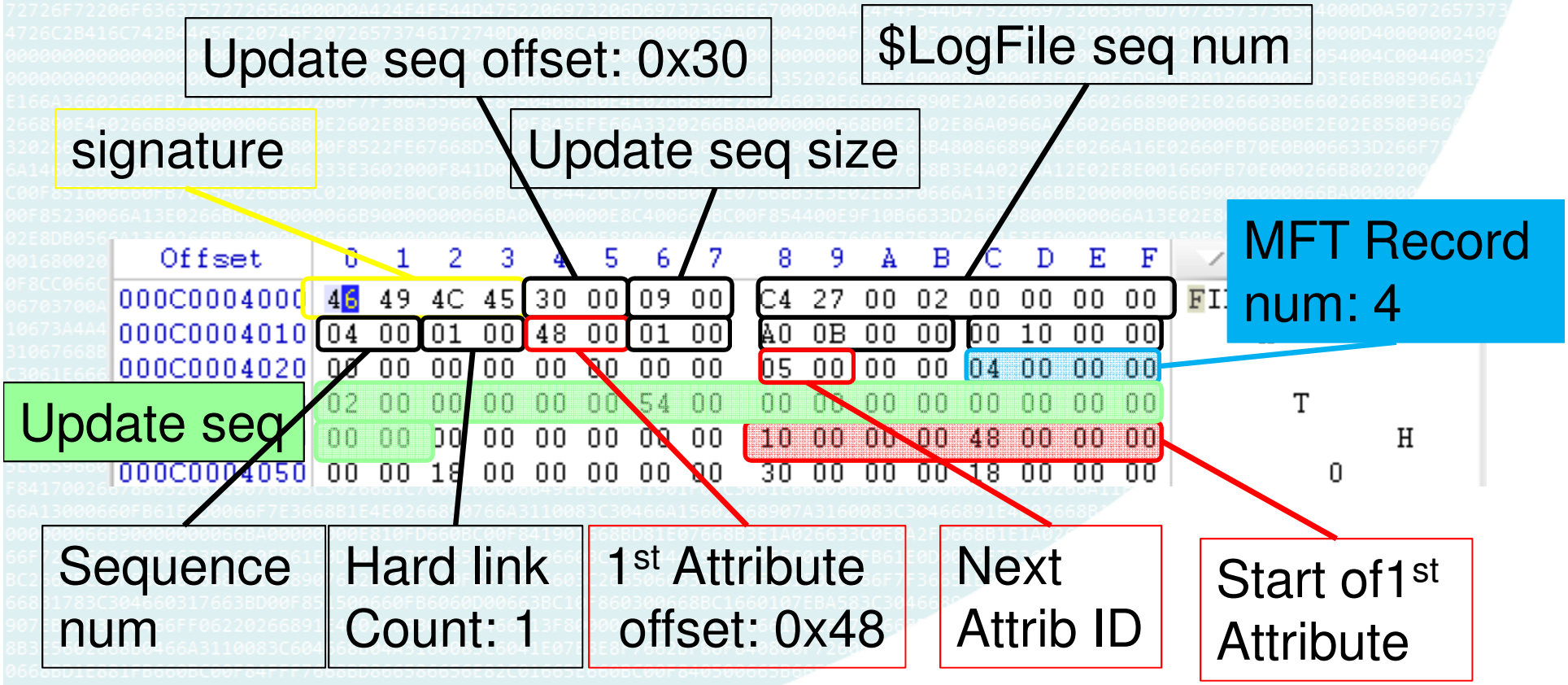
CHAMPLAIN COLLEGE

FILE_RECORD_SEGMENT_HEADER

- Next attrib ID – next ID to be allocated, tells us how many attributes to look for.

CHAMPLAIN COLLEGE

FILE_RECORD_SEGMENT_HEADER



CHAMPLAIN COLLEGE

Resident Attribute Header

Standard for all resident attributes

Name refers to attribute name, which is optional

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Type ID				Attribute Length				Form code	name len	Name offset		flags		Attrib ID	
1	Content length				Content offset		unused									

Source: http://msdn.microsoft.com/en-us/library/bb470039%28v=VS.85%29.aspx

Form code
0x00 = Resident
0x01 = Non resident

Flags
0x00FF = Compressed
0x8000 = Sparse
0x4000 = Encrypted

CHAMPLAIN COLLEGE

MFT Attributes - $AttrDef

ID	Attribute Type	Description
0x10	Standard Information	Includes information such as time stamp and link count.
0x20	Attribute List	Lists the location of all the attribute records that do not fit in the MFT record.
0x30	File Name	A repeatable attribute for both long and short file names. The long name of the file can be up to 255 Unicode characters. The short name is the MS-DOS-readable, 8.3, case-insensitive name for the file. Additional names, or hard links, required by POSIX can be included as additional file name attributes.
0x40	Object ID	A volume-unique file identifier. Used by the link tracking service. Not all files have object identifiers.
0x50	Security Descriptor	Shows information about who owns the file and who can access the file.
0x60	Volume Name	Used only in the $Volume system file. Contains the volume label.
0x70	Volume Information	Used only in the $Volume system file. Contains the volume version.
0x80	Data	Contains file data. NTFS allows multiple data attributes per file. Each file typically has one unnamed data attribute. A file can also have one or more named data attributes, each using a particular syntax.
0x90	Index Root	Used to implement folders and other indexes.
0xA0	Index Allocation	Used to implement folders and other indexes.
0xB0	Bitmap	Used to implement folders and other indexes.
0xC0	Reparse Point	Used for directory junction points and volume mount points. They are also used by file system filter drivers to mark certain files as special to that driver.
0x100	Logged Tool Stream	Similar to a data stream, but operations on a logged tool stream are logged to the NTFS log file just like NTFS metadata changes. Used by EFS.

Source: http://technet.microsoft.com/en-us/library/cc976808.aspx

CHAMPLAIN COLLEGE

$Standard_Information

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Date Created*								Date Modified							
10	Date MFT record modified								Date Accessed							
20	Flags				Max Versions				Version Num				Class ID			
30	Owner ID				Security ID				Quota Charged							
40	Update Sequence Number															

*Time values are in 100 nanoseconds since January 1, 1601 UTC

CHAMPLAIN COLLEGE

$Standard_Information flags

Bit	Meaning
0	Read only
1	Hidden
2	System
3	
4	
5	Archive
6	Device
7	Normal
8	Temporary
9	Sparse File
A	Reparse Point
B	Compressed
C	Offline
D	Not Indexed
E	Encrypted
F	

More information:
http://msdn.microsoft.com/en-us/library/aa365535(v=VS.85).aspx

CHAMPLAIN COLLEGE

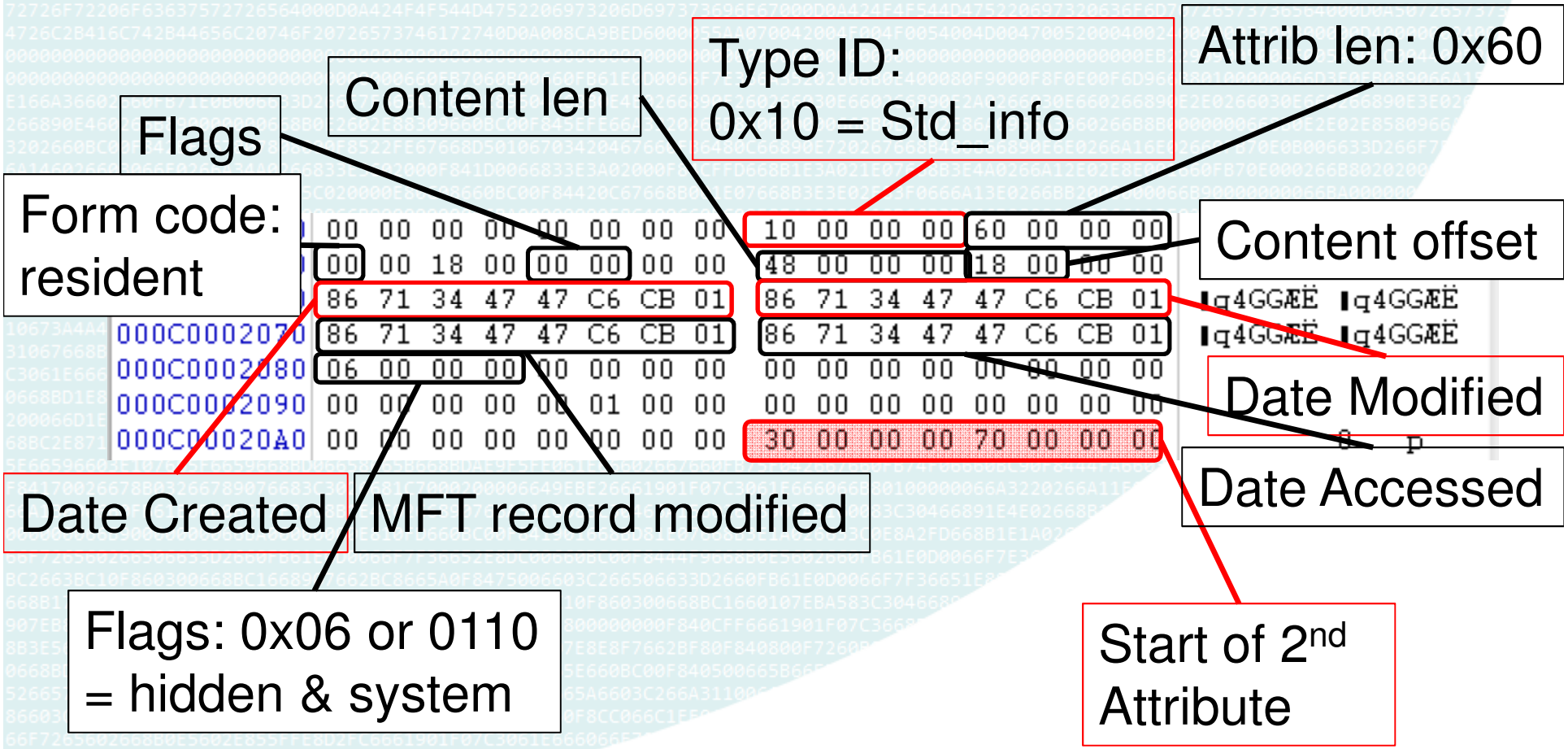
Standard Information Times

- Read by the NTFS driver
- Read by forensic tools
- Changed by timestomp
- Changed by MS SetFileTime function

http://msdn.microsoft.com/en-us/library/ms724933(v=VS.85).aspx

CHAMPLAIN COLLEGE

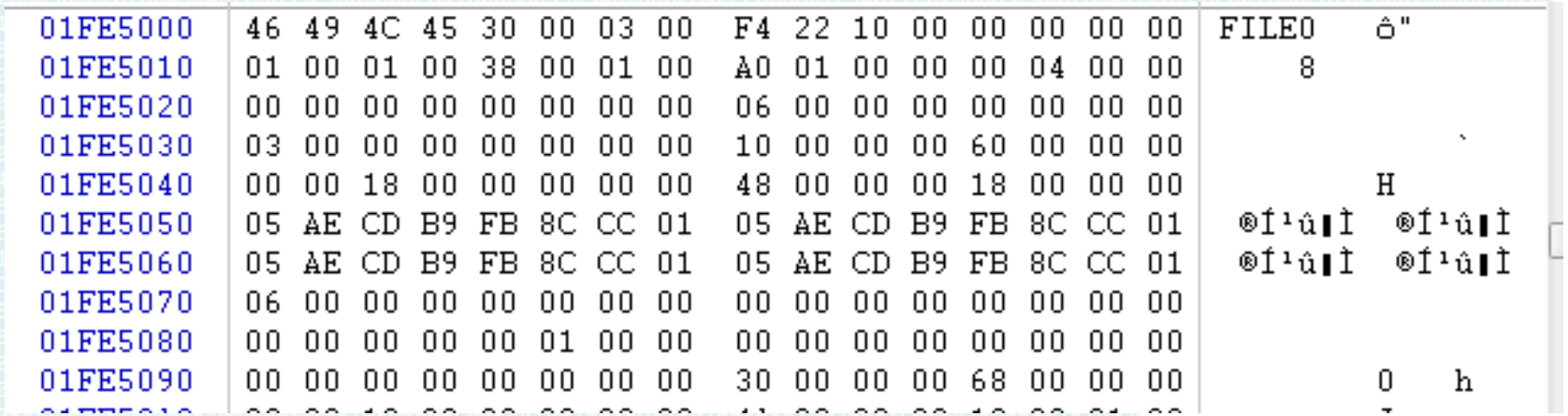
Practice $Standard_Information



CHAMPLAIN COLLEGE

Your turn 3

Decode first record entry on the $MFT on PFIC_01



01FE5000	46	49	4C	45	30	00	03	00	F4	22	10	00	00	00	00	00	FILE0 ô"
01FE5010	01	00	01	00	38	00	01	00	A0	01	00	00	00	04	00	00	8
01FE5020	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00	
01FE5030	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	`
01FE5040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00	H
01FE5050	05	AE	CD	B9	FB	8C	CC	01	05	AE	CD	B9	FB	8C	CC	01	®Í¹û▮Ì ®Í¹û▮Ì
01FE5060	05	AE	CD	B9	FB	8C	CC	01	05	AE	CD	B9	FB	8C	CC	01	®Í¹û▮Ì ®Í¹û▮Ì
01FE5070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01FE5080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	
01FE5090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	0 h

Use the data interpreter for the dates.

CHAMPLAIN COLLEGE

Your turn 3, solution

1st Attribute offset: 0x38

Flags: 0x01 In use

Size of MFT record: 0x01A0

MFT Record num: 0 ($MFT)

Next Attrib num

Attrib ID 0x10

Resident

Attrib Length 0x60

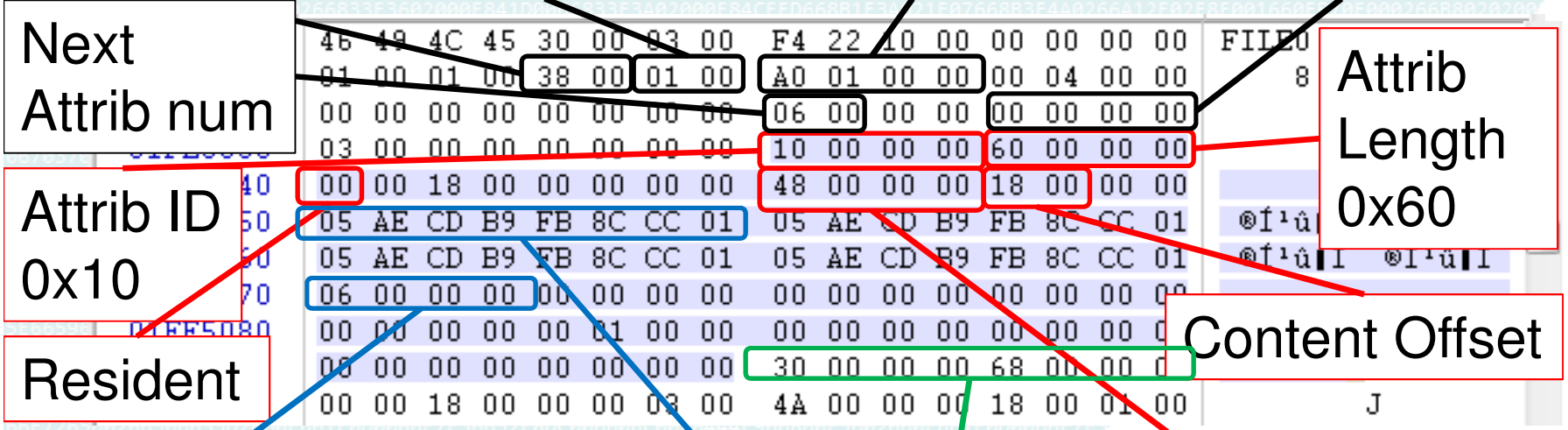
Content Offset

Flags 0x06 = 0110 = hidden & system

Date Created Oct 17, 2011

Content length

Next attribute type 0x30 = FileName



CHAMPLAIN COLLEGE

$File_Name

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Parent Directory								Date Created							
10	Date Modified								Date MFT Modified							
20	Date Accessed								Logical file size							
30	Size on disk								Flags*				Reparse value			
40	Name len	Name type	Name (variable length)													

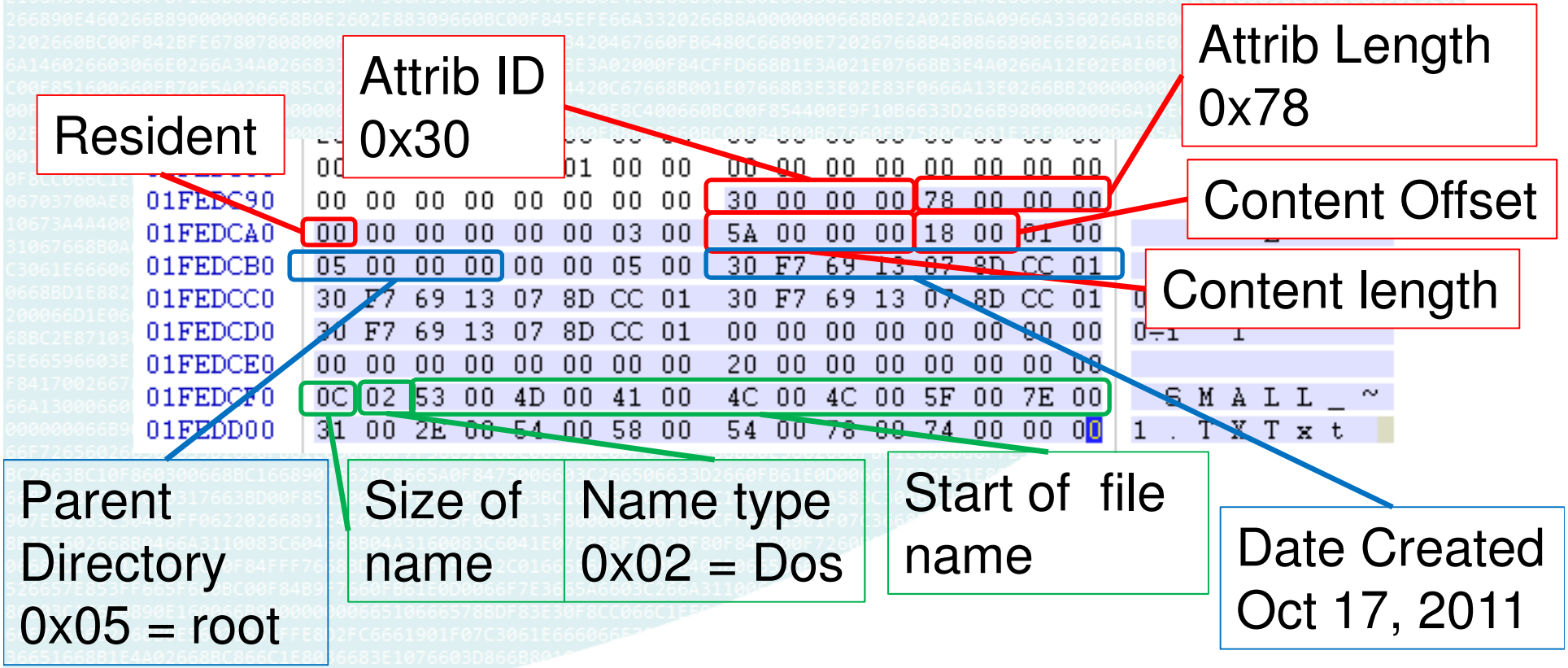
Name types

Value	Description
0	POSIX (unicode, case sensitive)
1	Win32 (unicode, case insensitive)
2	DOS (8.3 ASCII, case insensitive)
3	Win32 7 DOS (when Win32 fits in DOS space)

* Same meaning as $Standard_Information

CHAMPLAIN COLLEGE

Practice $File_Name



CHAMPLAIN COLLEGE

Non Resident Attribute Header

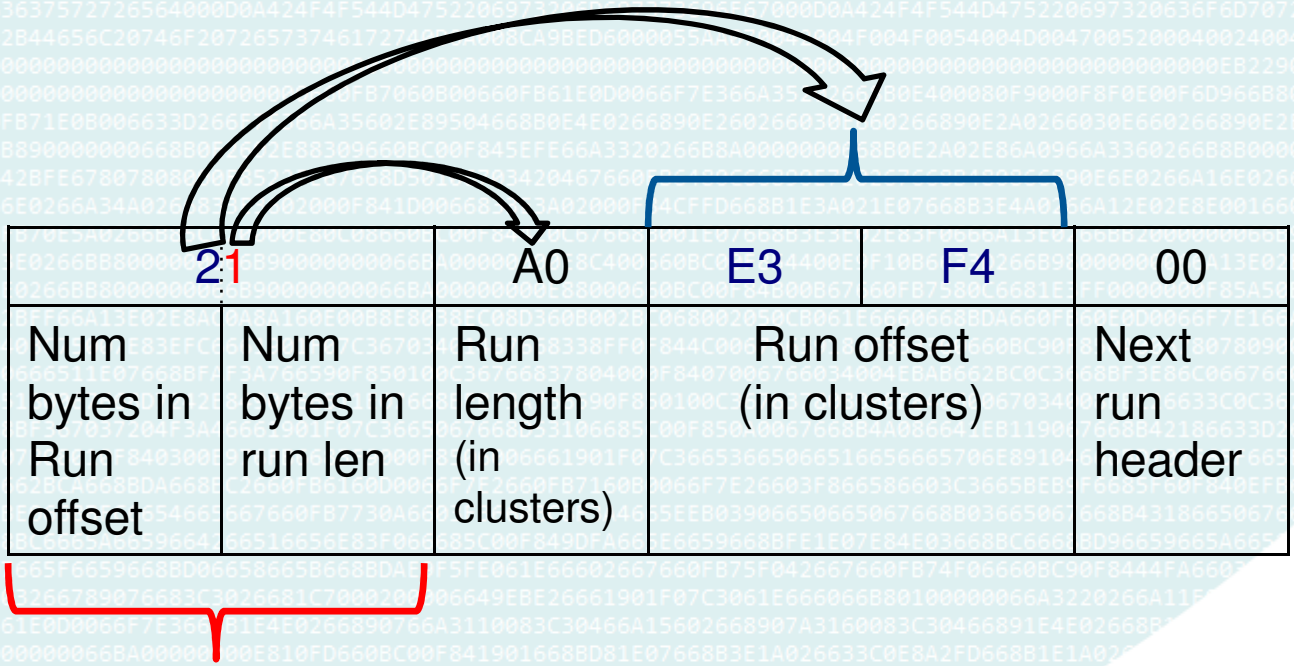
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Type ID				Attribute Length				Form code	name len	Name offset		flags		Atrib ID	
10	Start virtual cluster number								Ending virtual cluster number							
20	Runlist offset		Compression unit size		0x0000				Size of attribute content							
30	size on disk of attribute content								Initialized size of attribute content							
40	Data runlists															

Attrib ID starts from zero

Virtual cluster numbers are used when a MFT record is fragmented

CHAMPLAIN COLLEGE

Data runlists



CHAMPLAIN COLLEGE

Data runs, take 2

```
32 18 01 60 34 56 00
```

Run 1

Header = 0x32 = 2 byte len, 3 byte offset

Length = 0x0118

Offset = 0x563460

Start cluster = 0x563460, length of data = 0x118 clusters

CHAMPLAIN COLLEGE

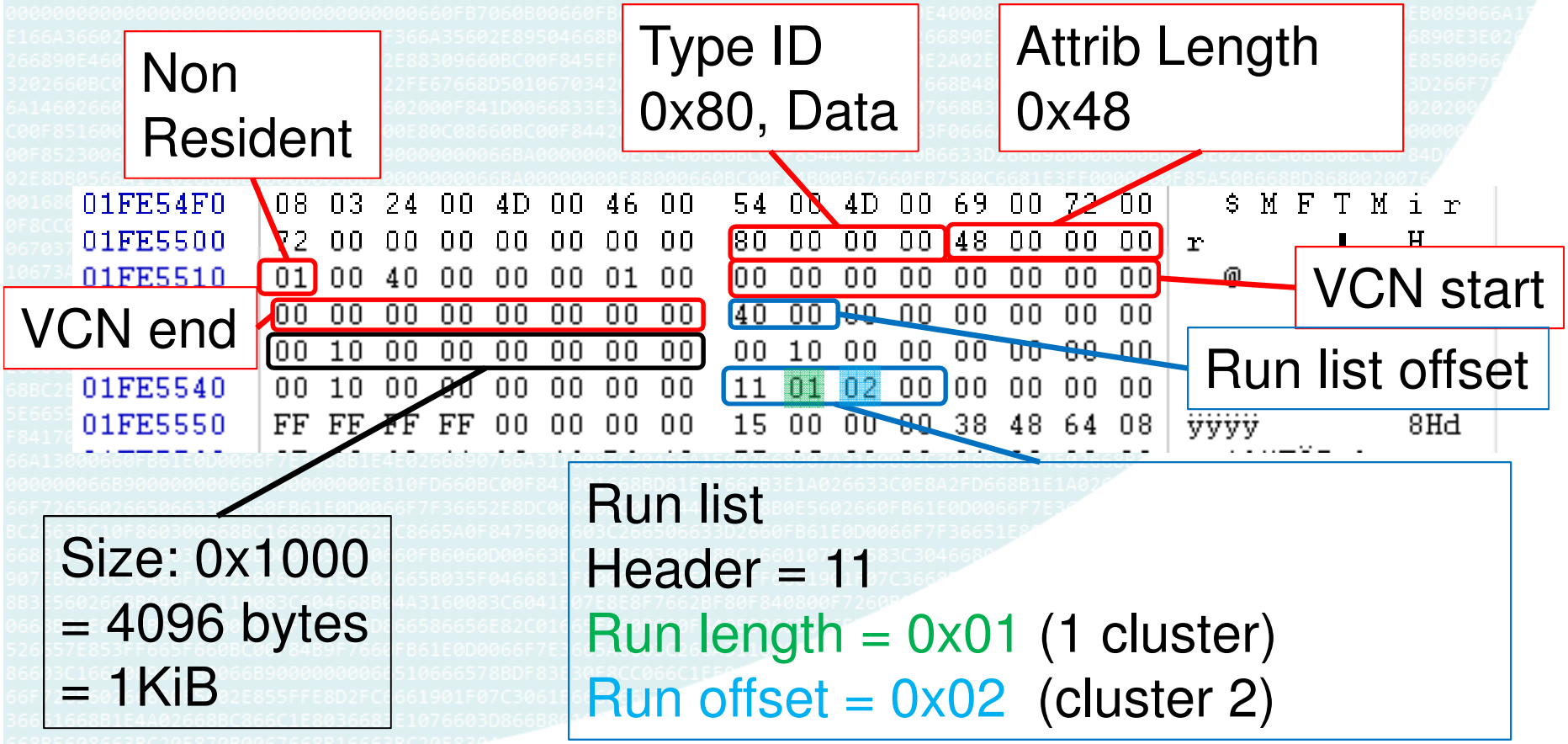
$Data

Standard header, with data run (if non resident)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Type ID 0x80				Attribute Length				Form code	name len	Name offset		flags		Atrib ID	
10	Start virtual cluster number								Ending virtual cluster number							
20	Runlist offset		Compression unit size		0x0000				Size of attribute content							
30	size on disk of attribute content								Initialized size of attribute content							
40	Data runlists															

CHAMPLAIN COLLEGE

Practice



CHAMPLAIN COLLEGE

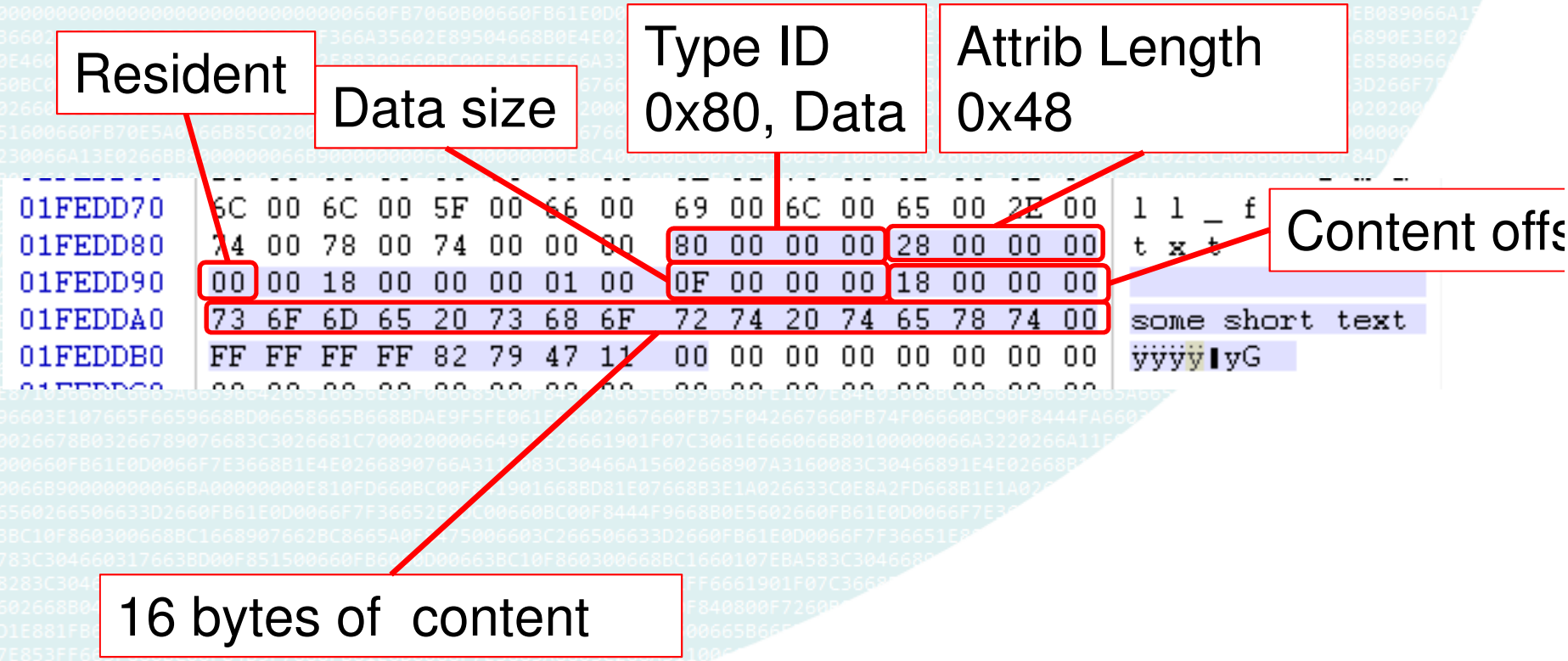
Your turn 4

Find the contents of the file named "small_file.txt" in PFIC_02.001

Hint: it is MFT record number 0x23

CHAMPLAIN COLLEGE

Resident Data



CHAMPLAIN COLLEGE

Your turn 5

Find the file named “big_file.txt” in PFIC_02.001

Hint: it is MFT record number 0x24

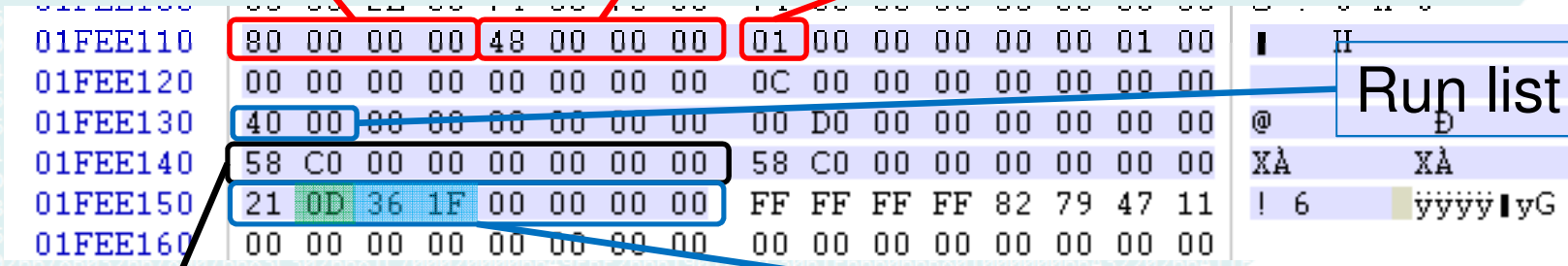
CHAMPLAIN COLLEGE

Non Resident data

Type ID
0x80, Data

Attrib Length
0x48

Non
Resident



Run list offset

Size:0xC058
= 49,240 bytes
= 48KiB

Run list
Header = 21
Run length = 0x0D (14 clusters, 53,248 bytes)
Run offset = 0x1F36
(=1F36x200x8=0x1F36000)

CHAMPLAIN COLLEGE

Additional Challenges

- PFIC_03.001
- Find:
  - Compressed directory and file
  - Directory with permissions set
  - Hidden directory
  - A directory that has been renamed

CHAMPLAIN COLLEGE

Thank you

- Todays exercises are at:
  http://www.writeblocked.org