University of Glasgow

Education and Training

By Dr. Wm. Bradley Glisson

Director Computer Forensics & E-Discovery MSc Program

The Value of Information

Information is an extremely valuable asset in the world's increasingly globally networked environment [1].

Cisco is predicting that annual global IP traffic will reach 667 Exabyte's by 2013 [3]

Cisco is also predicting that "Mobile data traffic will roughly double each year from 2008 to 2013" [3]

Education Impact

1. Traditional Digital Forensics Techniques

- Traditional Processes and Procedures
- Legal Issues

2. Internet Digital Forensics Techniques

- Browsers – Firefox / Internet Explorer / Chrome
- Instant message logs – Yahoo / Skype / MS IM
- Facebook, Twitter, Cloud Computing

3. Mobile Digital Forensics Techniques

- Traditional text messages
- Smart phones

Computer Forensic Process

1. Decide where to store the information
2. Counter data remembrance by wiping the drive
3. Document the hardware & Chain of Custody
4. Make a bit-stream copy of the removable media
5. Authenticate a forensic copy of the media
6. Conduct an analysis of the drive
7. Production of detailed documentation

File Systems

The file system is responsible for the organization of the files, i.e., it is responsible for the logical placement of the files on the storage drive.

- File system manipulates sectors so that they are treated as clusters
- Clusters are then manipulated so that they can store files

Understanding this interaction is critical to the retrieval of data that has been accidentally or intentionally deleted on various types of files systems like:

- File Allocation Table (FAT) system,
- New Technology File System (NTFS),
- High Performance File System (HPFS)
- Hierarchical File System (HFS)

Encryption

As encrypted documents become more prevalent how does the Archivist handle this situation?

- FTK's PRTK

How do you handle a drive that has Bit Locker implemented?

- Find the Recovery Key and/or Startup Key
- The user is prompted to insert the USB flash drive that holds the recovery key and/or start-up key.
- For recovery purposes, BitLocker uses the Recovery Key (a key used for recovering data encrypted on a BitLocker volume) or the Recovery Password (numerical password), so that an authorized user can still access the system in case of a security, hardware, or other failure.

University of Glasgow

Skype IM

Skype™ - Options

General
General Settings
Audio Settings
Sounds
Video Settings
Privacy
Notifications
Calls
Chats & SMS
Advanced

Video Settings: set up your webcam

Enable Skype Video
Start my video automatically when I am in a call
Select webcam:
Default video device
Webcam Settings

No webcam found. Connect your webcam or check it is properly connected.

Automatically receive video from...
anyone
only people in my Contact List
no one

Show that I have video to...
people in my Contact List
no one

Other things you can do
Learn more about setting up your webcam
Buy a web camera from the Skype Shop

Save
Cancel

Skype™ - Options

General
Privacy
Privacy Settings
Blocked Users
Notifications
Calls
Chats & SMS
Advanced

Privacy Settings: protect yourself from unwanted calls and chats

Allow calls from...
anyone
only people in my Contact List

Automatically receive video from...
anyone
only people in my Contact List
no one

Show that I have video to...
people in my Contact List
no one

Allow chats from...
anyone
only people in my Contact List

Keep chat history for
forever
Clear Chat History

Allow my status to be shown on the web. Learn more
Accept Skype Browser Cookies Learn more
Clear Skype Cookies

Show Basic Options

Save
Cancel

User Information

C:\Documents and Settings\C*omputer_Id*\Application Data\Skype\brad.glisson

Phone Call Records

File Transfer Activity

Display Icons

Contact List

Voice Messages

Profile Information

Log file indicates the type of data being tracked and the size of the log

Chatmsg256.dbb

Chatmsg512.dbb

Chatmsg1024.dbb

Chatmsg2048.dbb

Chatmsg4096.dbb

The numbers represent the size of the record entry not the actual file size

Profile Information (Profile 256.dbb)

AccessData Forensic Toolkit Version: 2.2.0.624 Database: localhost Case: Brad - Skype

File Edit View Evidence Filter Tools Help

Filter: - unfiltered - Define...

Explore | Overview | Email | Graphics | Bookmarks | Live Search | Index Search | NEW TAB!!! | Glisson

Evidence Items

- Evidence
  - SKYPE Information - C:\Documents and Settings\wbg1n\Desktop\SKYPE Informatior
    - Skype
      - brad.glisson
        - chatsync
        - dyncontent
        - httpfe
        - voicemail
      - Content
      - dr.glisson
      - glisson
      - global_traveller
      - Pictures

File Content

Hex | Text | Filtered | Natural

```
00 6c 33 33 6c bd 00 00 00-0c 00 00 00 41 14 00 09 | l33l½·····A···
10 05 03 14 42 72 61 64 20-47 6c 69 73 73 6f 6e 00 | ···Brad Glisson·
20 03 30 47 6c 61 73 67 6f-77 00 03 94 18 00 00 85 | ·0Glasgow·····
30 05 02 00 81 05 02 03 24-65 6e 00 03 28 67 62 00 | ·····$en··(gb·
40 03 a8 02 47 42 50 00 00-ad 02 a7 04 00 4d 9c 98 | ·¨·GBP···-·§··M··
50 87 c5 04 00 0b 02 04 07-23 00 00 00 02 62 2e 67 | ·Å·····#····b.g
60 6c 69 73 73 6f 6e 40 68-61 74 69 69 2e 61 72 74 | lisson@hatii.art
70 73 2e 67 6c 61 2e 61 63-2e 75 6b 00 03 10 62 72 | s.gla.ac.uk···br
80 61 64 2e 67 6c 69 73 73-6f 6e 00 00 9d 05 00 03 | ad.glisson·····
90 40 62 2e 67 6c 69 73 73-6f 6e 40 68 61 74 69 69 | @b.glisson@hatii
a0 2e 61 72 74 73 2e 67 6c-61 2e 61 63 2e 75 6b 00 | .arts.gla.ac.uk·
b0 00 6d 80 a3 05 03 74 75-6b 00 00 85 19 bb cb d7 | ·m·£··tuk····»Ë×
c0 09 00 99 05 00                                  | ·····
```

Cursor pos = 0

File Content | Properties | Hex Interpreter

File List

Normal

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
$I30		1015	<missin...	SKYPE Information/C:\D...	Index ...	n/a	8192 B	492006...	962D1...		12/08/2008 19:...	20/02/2010 19:...	19/02/2010 18:...
call256.dbb		1016	dbb	SKYPE Information/C:\D...	INSO U...	n/a	114.8 KB	3BA3C...	C169F...		15/08/2008 14:...	20/02/2010 19:...	16/02/2010 19:...
callmember256.dbb		1017	dbb	SKYPE Information/C:\D...	INSO U...	n/a	115.8 KB	A09B6...	A9C5E...		15/08/2008 14:...	20/02/2010 19:...	18/02/2010 19:...
chat256.dbb		1018	dbb	SKYPE Information/C:\D...	Zero Le...	n/a	0 B				14/02/2010 16:...	14/02/2010 17:...	14/02/2010 17:...
chat512.dbb		1019	dbb	SKYPE Information/C:\D...	INSO U...	n/a	85.75 KB	96273...	3C924...		15/08/2008 11:...	20/02/2010 19:...	16/02/2010 11:...
chatmember256.dbb		1020	dbb	SKYPE Information/C:\D...	INSO U...	n/a	86.72 KB	9DC18...	D1ADD...		15/08/2008 11:...	20/02/2010 19:...	14/02/2010 18:...
chatmsg1024.dbb		1021	dbb	SKYPE Information/C:\D...	INSO U...	n/a	64.02 KB	BD53B...	525538...		25/09/2008 19:...	20/02/2010 19:...	13/02/2010 20:...
chatmsg2048.dbb		1022	dbb	SKYPE Information/C:\D...	INSO U...	n/a	13.14 KB	D9B22...	B69AF...		31/10/2008 15:...	20/02/2010 19:...	23/11/2009 14:...
chatmsg256.dbb		1023	dbb	SKYPE Information/C:\D...	INSO U...	n/a	620.8 KB	175905...	1D08F...		15/08/2008 11:...	20/02/2010 19:...	14/02/2010 18:...
chatmsg4096.dbb		1024	dbb	SKYPE Information/C:\D...	INSO U...	n/a	11.34 KB	56FDA...	1E8E26...		21/09/2008 15:...	20/02/2010 19:...	05/05/2009 12:...
chatmsg512.dbb		1025	dbb	SKYPE Information/C:\D...	INSO U...	n/a	114.1 KB	ABD79...	42B0C...		20/08/2008 10:...	20/02/2010 19:...	14/02/2010 18:...
chatsync		1026		SKYPE Information/C:\D...	Folder	n/a	0 B				15/08/2008 11:...	20/02/2010 19:...	20/02/2010 19:...
config.lck		1027	lck	SKYPE Information/C:\D...	Zero Le...	n/a	0 B				12/08/2008 19:...	27/10/2009 10:...	12/08/2008 21:...
config.xml		1028	xml	SKYPE Information/C:\D...	XML	n/a	25.69 KB	D0E7F...	F3725E...		12/08/2008 19:...	20/02/2010 19:...	19/02/2010 18:...
config.xml.copy0		1029	copy0	SKYPE Information/C:\D...	INSO U...	n/a	25.69 KB	C7EFB...	CAD98...		12/08/2008 19:...	20/02/2010 19:...	19/02/2010 12:...

Lots of Issues in Mobile forensics

- **Manufactures constantly updating and changing firmware**
- **Manufactures changing the way individual makes and models handled memory storage**
- **Different manufactures approach to memory storage**
- **Increasing phone functionality - Pace of Technology**
  - iPhone overtaken by Android in the US
  - Mobile forensics is rapidly becoming a hot topic in the global digital forensics environment. This is, largely, due “to 4.1 billion mobile subscriptions in the world, a global penetration rate of 61.1 percent” .

    Pearce, James Quintana. *Report: 4.1 Billion Mobile Subscribers Worldwide Helps Reduce Digital Divide (Slightly)* http://moconews.net/article/419-4.1-billion-mobile-subscribers-mobile-helping-reduce-digital-divide-sli/.
  - Couple this information with the fact that the iPod Touch [15] and the iPhone are becoming part of the military issued kit.

    Mark, Roy. *Military Coders Deploy iPod Touch, iPhone on Duty*. http://www.pdfzone.com/.

Questions

- **Does the archivist have an obligation to recover as much information as is possible from the digital media?**
- **Does the increase of quantity of data potentially contribute to the an increase in knowledge in the field of Digital Curation?**
- **Under what conditions would it be beneficial for collecting institutions to copy entire drives, i.e. all of the bits, rather than only copying the live files from the drives?**
- **Are current practices of collecting institutions practical from a business perspective?**
- **How often, and under what conditions, will the processes and storage arrangements of collecting institutions need to be upheld in a court of law?**

Education Impact

1. Traditional Digital Forensics Techniques

- Traditional Processes and Procedures
- Legal Issues

2. Internet Digital Forensics Techniques

- Browsers – Firefox / Internet Explorer / Chrome
- Instant message logs – Yahoo / Skype / MS IM
- Facebook, Twitter, Cloud Computing

3. Mobile Digital Forensics Techniques

- Traditional text messages
- Smart phones

Contact Details

Brad Glisson, Ph.D.

Course Director & Lecturer in Computer Forensics and E-Discovery

Humanities Advanced Technology and Information Institute (HATII)

University of Glasgow

George Service House

11 University Gardens

Glasgow, G12 8QQ

Tel: +44 (0)141 330 8591

Email: b.glisson@hatii.arts.gla.ac.uk

Web Page: http://www.hatii.arts.gla.ac.uk/staff/bg.html

University of Glasgow

Hardware Documentation & Chain of Custody

Documentation of the handling of original media

Where it was stored?

Who had access to it?

What was done to it?

- No information has been added, deleted or altered in the copying or analysis
- A complete copy of the evidence is made and verified
- A reliable copying process is used
- Ensure all relevant data is copied
- All media is secured

Serial Numbers & Manufacture Information & any information displayed on the outside of the drive

The idea is to provide documentation demonstrating preservation of data integrity.

Computer Forensic Process

1. Decide where to store the information
2. Counter data remembrance by wiping the drive
3. Document the hardware & Chain of Custody
4. **Make a bit-stream copy of the removable media**
5. **Authenticate a forensic copy of the media**
6. Conduct an analysis of the drive
7. Production of detailed documentation

Bit Stream Copy & Authentication

A bit-stream copy of the removable media copies every bit on the source drive.

- Clone – bootable copy of the drive
- Forensic Image - bit-stream copy is saved to an image file

Authentication - typically done through the execution of a one-way hash on both devices to verify that they are identical

- Hashes are used to uniquely identify a specific file. The hash value generated from a file becomes its “digital fingerprint”.
- Message-Digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA) are the two most common hash algorithms used in computer forensics.

References

1. Glisson, W.B. and R. Welland. *Web Development Evolution: The Assimilation of Web Engineering Security*. in *3rd Latin American Web Congress*. 2005. Buenos Aires - Argentina: IEEE CS Press.

2. Aitoro, J.R. *Administration faces big challenge in records preservation*. 2008 [cited 2009 Januaruy 17]; Available from: http://www.govexec.com.

3. Cisco - http://newsroom.cisco.com/dlls/2009/prod_060909.html

4. Department of Defense, *National Industry Security Program Operating Manual*, D.o. Defense, Editor. 2006, Defense Technical Information Center: Washington, DC.

5. Defense Security Service. *Industry Security Letter*. 2007 [cited 2009 Jan. 17]; Available from: https://www.dss.mil/.

6. Wright, C., D. Kleiman, and S. Sundhar, *Overwriting Hard Drive Data: The Great Wiping Controversy*, in *Information Systems Security*. 2008, Springer Berlin / Heidelberg. p. 243-257.

7. http://www.informit.com/articles/article.aspx?p=339042

Wipe Target Drive

Many companies promote a US Department of Defense (DOD) standard on this topic. However, the 2006 National Industry Security Program Operating Manual (that is also referenced as the DOD 5220.22-M) does not specify the number of passes required to achieve sanitation [4].

Defense Security Service (DSS) - "DSS will no longer approve overwriting procedures for the sanitization or downgrading (e.g. release to lower level classified information controls) of IS storage devices (e.g., hard drives) used for classified processing" [5]

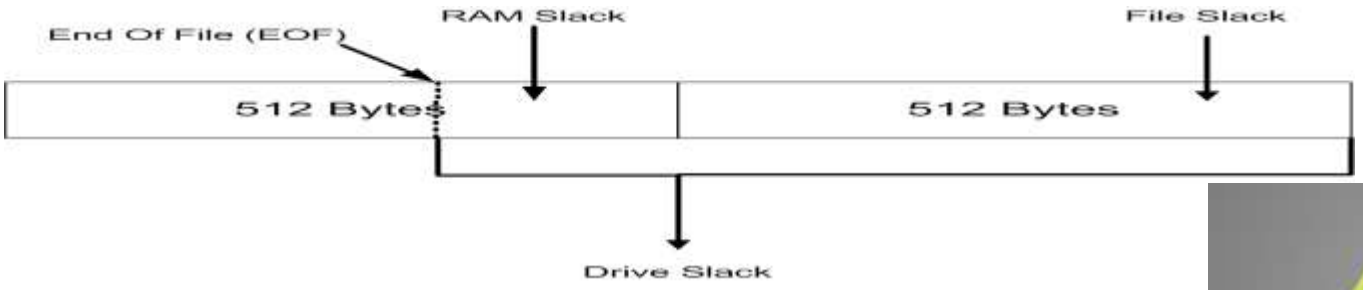
Current Research "…that correctly wiped data cannot reasonably be retrieved even if it is of a small size or found only over small parts of the hard drive" [6]

Drive Analysis and Detailed Reporting

Active files are readily identifiable and can be accessed with the appropriate software and, in some cases, the required security information.

Inactive files can be located by carving the unallocated space and slack space off of the drive.

- Cluster - Grouping of sectors used to save data by the OS.
- Drive Slack - Composed of unused space in a cluster between the end of an active file and the end of a cluster
- Ram Slack - Composed of the unused space between the end of the File (EOF) and the end of the sector
- File Slack - Comprised of unused space in sectors until the end of the cluster (EOC)



Documentation - All Issues & Evidence Discovered

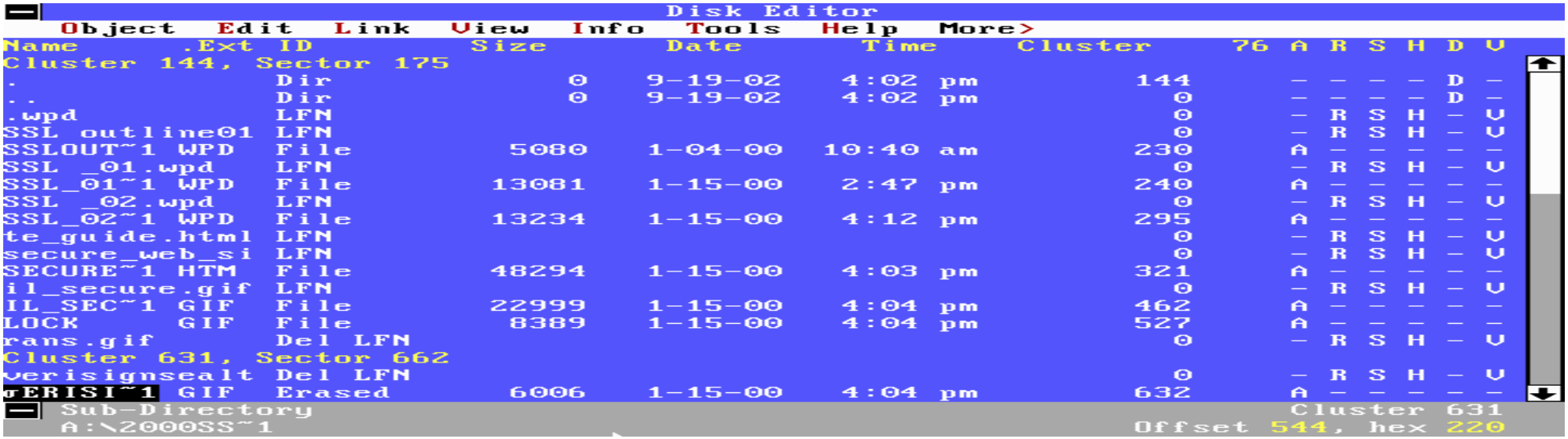
Data Keys Commonly Use FAT

Deletion of a file:

1.The first character of the file is replaced with a non-readable character

2.The FAT entries linking the sector clusters are zeroed out.

If additional data has been saved to the system after a file has been deleted, the old data may have been over written.



Disk Editor

Object Edit Link View Info Tools Help More>

Name	.Ext	ID	Size	Date	Time	Cluster	76	A	R	S	H	D	V
Cluster 144, Sector 175													
.		Dir	0	9-19-02	4:02 pm	144		-	-	-	-	D	-
..		Dir	0	9-19-02	4:02 pm	0		-	-	-	-	D	-
.wpd		LFN				0		-	R	S	H	-	V
SSL outline01		LFN				0		-	R	S	H	-	V
SSLOUT~1	WPD	File	5080	1-04-00	10:40 am	230		A	-	-	-	-	-
SSL _01.wpd		LFN				0		-	R	S	H	-	V
SSL_01~1	WPD	File	13081	1-15-00	2:47 pm	240		A	-	-	-	-	-
SSL _02.wpd		LFN				0		-	R	S	H	-	V
SSL_02~1	WPD	File	13234	1-15-00	4:12 pm	295		A	-	-	-	-	-
te_guide.html		LFN				0		-	R	S	H	-	V
secure_web_si		LFN				0		-	R	S	H	-	V
SECURE~1	HTM	File	48294	1-15-00	4:03 pm	321		A	-	-	-	-	-
il_secure.gif		LFN				0		-	R	S	H	-	V
IL_SEC~1	GIF	File	22999	1-15-00	4:04 pm	462		A	-	-	-	-	-
LOCK	GIF	File	8389	1-15-00	4:04 pm	527		A	-	-	-	-	-
rans.gif		Del LFN				0		-	R	S	H	-	V
Cluster 631, Sector 662													
verisignsealt		Del LFN				0		-	R	S	H	-	V
ERISI~1	GIF	Erased	6006	1-15-00	4:04 pm	632		A	-	-	-	-	-

Sub-Directory Cluster 631

A:\2000SS~1 Offset 544, hex 220

Future Research

- **Examination of the current process used in the field of digital curation**
  - Conducting survey inquiries with collecting institutions in several different countries.
  - The investigation and development of a digital recovery methodology specifically for use in digital curation.
  - A targeted educational effort toward librarians and archivists on relevant tools and the operation of specific file systems
  - Followed by empirical studies of the practicality and effectiveness of the developed methodologies to meet the needs of collecting institutions and their target user communities

C:\Documents and Settings\wbg1n\Application Data\Skype\brad.glisson

File Edit View Favorites Tools Help

Back Search Folders

Address C:\Documents and Settings\[redacted]\Application Data\Skype\brad.glisson Go

Folders

- Adobe
- Apple Computer
- ATI
- CyberLink
- Elluminate
- EndNote
- Free Download Manager
- geany
- gnupg
- gtk-2.0
- Help
- Identities
- InstallShield
- Macromedia
- Mael
- Microsoft
- Mozilla
- NCH Swift Sound
- Real
- Skype
  - brad.glisson
    - chatsync
    - dyncontent
    - httpfe
    - voicemail
  - Content
  - dr.glisson

chatsync	dyncontent	httpfe	voicemail
call256.dbb DBB File 115 KB	callmember256.dbb DBB File 116 KB	chat512.dbb DBB File 86 KB	chatmember256.dbb DBB File 87 KB
chatmsg256.dbb DBB File 621 KB	chatmsg512.dbb DBB File 115 KB	chatmsg1024.dbb DBB File 65 KB	chatmsg2048.dbb DBB File 14 KB
chatmsg4096.dbb DBB File 12 KB	config.lck LCK File 0 KB	config.xml XML Document 26 KB	contactgroup256.dbb DBB File 3 KB
index2.dat DAT File 66 KB	profile256.dbb DBB File 0 KB	profile4096.dbb DBB File 4 KB	user256.dbb DBB File 1 KB
user1024.dbb DBB File 9 KB	user4096.dbb DBB File 17 KB	user16384.dbb DBB File 101 KB	voicemail256.dbb DBB File 1 KB