THE EVIDENCE IS IN ELECTRONIC FORM

“To say electronically stored information (ESI) is on the rise would be a glaring and obvious understatement. But it is also true. The fact is over 95% of corporate information is now digital and more ESI is created each 15 minutes than all written data penned from the beginning of time through the year 2004.

- Michael Swarz
What is Computer Forensics?
...is it the same as E-Discovery?

“Computer Forensics is the use of specialized techniques for recovery, authentication and analysis of electronic data when an investigation or litigation involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel, and generally requires strict adherence to chain-of-custody protocols.” – Sedona Conference Glossary

E-Discovery is “The process of collecting, preparing, reviewing, and producing electronically stored information (“ESI”) in the context of the legal process.” – Sedona Conference Glossary
Computer Forensics is the use of specialized techniques for recovery, authentication and analysis of electronic data when an investigation or litigation involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel, and generally requires strict adherence to chain-of-custody protocols.

– Sedona Conference Glossary

E-Discovery is "The process of collecting, preparing, reviewing, and producing electronically stored information ("ESI") in the context of the legal process."

– Sedona Conference Glossary

What is Computer Forensics?...isn't it just E-Discovery? We get it.
Computer Forensics – Example Cases

- Theft of Trade Secrets
- Non-Compete / Non-Solicitation
- Workplace Harassment
- Unauthorized Access (hacking)
- Document Metadata Examination
Key Considerations

ESI is Fragile – it is easy to change or delete

That is why we:
• Don’t work from the original evidence unless necessary
• Make a verified copy (x2)
• Document it with chain of custody, photos and other identifiable characteristics
• Use appropriate tools and methods
### Where Does the Electronic Evidence Come From?

...Everywhere You Can Imagine

<table>
<thead>
<tr>
<th>Computers</th>
<th>Social Media</th>
<th>Cloud</th>
<th>Security Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Laptops</td>
<td>• Facebook</td>
<td>• Office 365</td>
<td>• Firewall</td>
</tr>
<tr>
<td>• Desktops</td>
<td>• Twitter</td>
<td>• Gmail</td>
<td>• IDS/IPS</td>
</tr>
<tr>
<td>• Business Class Servers</td>
<td>• LinkedIn</td>
<td>• Salesforce</td>
<td>• SIEM</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Phones</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tablets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• GPS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Wearables</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Specialized equipment and software tools are used to prevent changes to the source media or data. There is often more than one way to perform the “copy” process, depending on the needs of the case.

The tools utilize hash algorithms to establish the copy made matches the original.
Not what you might be thinking...

A hash value is the unique value, sometimes called “digital signature,” associated with a piece of media or data file after being processed through a hashing algorithm such as MD5 or SHA-1.

The purpose is to identify if any changes have been made during the copy process and to use the hash to identify exact duplicates.
What is a Hash?

The quick brown fox jumps over the lazy dog.
MD5 Hash Value: e4d909c290d0fb1ca068ffaddf22cbd0

The quick brown fox jumps over the lazy log.
MD5 Hash Value: 269615d22954c4829f46258103deedeb
Time to examine the data, but it doesn't look like you might think.

Forensic analysis takes specialized techniques and tools. It most certainly doesn't look as friendly or intuitive to review as the computer does to a typical user.
Examination may include the review of both active data and deleted data. Even files that are corrupt, encrypted or fragments of the original file can be useful during a forensic exam.
Artifacts Most Commonly Examined

- Registry Hives
- Prefetch
- LNK / Jumplist
- Internet Browser Files
- Recycle Bin
- Hard Drive’s File System
- Operating System Log Files
- Application Specific Log Files
- Unallocated Space

...and finally, the content of the files themselves.
Raw Data is Not Intuitive

A key role of a forensic examiner is to distill complex or confusing technical data down to meaningful and actionable results.
Provide information that can be understood. Not technical jargon where it isn’t needed.

<table>
<thead>
<tr>
<th>Description</th>
<th>Serial Number</th>
<th>First Recognized - EST</th>
<th>Last Recognized - EST</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADATA USB Flash Drive</td>
<td>1453015892566005F</td>
<td>02/19/2016 08:25:32 AM</td>
<td>02/19/2016 08:25:35 AM</td>
</tr>
<tr>
<td>Seagate FreeAgent Go</td>
<td>2LE90G62</td>
<td>06/25/2014 10:05:42 AM</td>
<td>02/16/2016 02:09:25 PM</td>
</tr>
<tr>
<td>WD My Passport 0820</td>
<td>57584831454334867533</td>
<td>07/04/2014 08:15:18 PM</td>
<td>02/12/2016 12:05:14 PM</td>
</tr>
<tr>
<td>WD My Passport 0748</td>
<td>57584335675300383931</td>
<td>06/12/2015 03:37:13 PM</td>
<td>01/29/2016 02:22:16 PM</td>
</tr>
<tr>
<td>Seagate FreeAgent Go</td>
<td>2GE32KNH</td>
<td>06/12/2015 05:39:32 PM</td>
<td>01/28/2016 10:57:52 PM</td>
</tr>
<tr>
<td>ADATA USB Flash Drive</td>
<td>1452821002587992</td>
<td>07/29/2014 10:41:54 PM</td>
<td>08/03/2015 02:42:28 PM</td>
</tr>
<tr>
<td>WD My Passport 070A</td>
<td>57583530A67873C37353</td>
<td>06/15/2014 10:28:19 PM</td>
<td>07/19/2015 10:39:30 PM</td>
</tr>
<tr>
<td>SanDisk Cruzer</td>
<td>20052255279866005172</td>
<td>06/15/2015 10:33:15 PM</td>
<td>07/10/2015 09:48:58 PM</td>
</tr>
<tr>
<td>PNY USB 2.0 FD</td>
<td>86795264389221</td>
<td>06/21/2015 03:06:14 PM</td>
<td>06/27/2015 07:06:15 PM</td>
</tr>
</tbody>
</table>
Purpose of prefetch files is to speed up launching applications.

Forensic examiners review these files for the purpose of determining recent application usage. Data destruction tools or other unauthorized applications may leave behind evidence of their use within prefetch files.
Recycle Bin
... all those things you thought you got rid of

When a file is sent to the Recycle Bin it is renamed and a record is created containing info about the file.

- **$I files** contain the info regarding what was deleted (original name, path, deletion date/time, size)
- **$R files** are the actual deleted files

Can be emptied (destroys the $R files) but may still contain the records of what was there.
LNK Files and Jump Lists

Exist to provide quicker access to “recent” files, folders and applications.

Provides an examiner a robust history of when, where and what was opened by each user.
Allocated vs Unallocated

.... the stuff your computer forgets

Active files = allocated
The operating system and hard drive track and know data is stored in that specific location.

Each file has a record in the Master File Table (“MFT”) which tracks where it is on disk and attributes about the file. e.g. when it was created, modified, etc

Deleted files = unallocated
The operating system and hard drive “forget” about the data stored in that specific location but that doesn’t mean it’s gone...

When a file is deleted the space it occupied becomes “unallocated,” that is, the MFT and therefore the drive, considers that space useable. However, as mentioned before, the data isn’t truly gone until it is overwritten.
Why Does Unallocated Space Matter?

Sounds good, talk then.

On Thu, Nov 22, 2013 at 8:03 AM, Jim Smith wrote:

Sam, let's talk at 10:30am heading into a meeting.

Chat soon,

Regards,

Jim Smith

Vice President of HR

Your Biggest Competitor Inc

On Nov 22, 2013, at 7:27 AM, Sam Smith wrote:

Jim,

Sorry I couldn't call last night.

Thanks,

Sam
Why Does Unallocated Space Matter?

Because that deleted data might not be gone!

Sounds good, talk then.

On Thu, Nov 22, 2013 at 8:03 AM, Jim Smith wrote:

On Nov 22, 2013, at 7:27 AM, Sam Smith wrote:

Sorry I couldn't call last night.

Does 8 AM work on your end?

Thanks,
Why Does Unallocated Space Matter?

This is just one example of an email conversation that took place on Gmail, never “downloaded” in email form to the computer via Outlook. It was simply viewed in the web browser and the internet history was deleted.

...it was still recovered, 5 months later.
Depending on the needs of the client the report could be in many forms:

- Oral report, in person or on the phone
- Email summary with attachments
- Formal “letter” style
- Declaration or Affidavit
Case Examples

California Court Enters Preliminary Injunction for Trade Secret Theft against Former Employee of Global Manufacturer of Fire and Gas Monitoring Systems: bit-x-bit Provides Forensic Analysis and Supporting Declaration

General Monitors, Inc. v. Detectors, Incorporated and Wing Lam, Case No. 30-2-16-00865073

State of Washington: TRO Entered under Federal Defend Trade Secrets Act against Two Former Employees of National Roofing Company: bit-x-bit Provides Forensic Analysis and Supporting Declaration

CentiMark Corporation v. Executive Roof Services, LLC, Michael W. Meacham, and Eric S. Pauly, Case No. 3:16-cv-05707
CENTIMARK CORPORATION, a Pennsylvania corporation,

Plaintiff,

vs.

EXECUTIVE ROOF SERVICES, LLC, a Washington limited liability company; MICHAEL W. MECHAM, an individual; and ERIC S. PAULY, an individual,

Defendants.

Case No.: 3:16-cv-05707

DECLARATION OF BRETT CREASY IN SUPPORT OF PLAINIFF’S MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION
13. As part of my analysis, the internet history on the Pauly computer was also analyzed. This analysis revealed that on July 23, 2016, the date I understand Pauly resigned from CentiMark, he conducted a Google search for “how to wipe a hard drive” and subsequently visited two websites which describe the process. Attached hereto as Exhibit H is a screenshot showing Pauly’s internet browsing history and the visit of these sites on July 22, 2016 starting at 11:24 p.m. Wiping a computer is a process by which the user destroys all documents and files present on the computer, including the operating system, and renders them unrecoverable. Based on the deletion activity discussed in the sections above, it appears Pauly chose to delete documents found on his CentiMark issued computer.
Brett Creasy
Vice President & Director of Digital Forensics

bit-x-bit, LLC
437 Grant Street, Suite 1250
Pittsburgh, Pennsylvania 15219

412-325-4033
info@bit-x-bit.com