Annual ADFSL Conference on Digital Forensics, Security and Law

2007
Proceedings

Towards Redaction of Digital Information from Electronic Devices

Gavin W. Manes
Oklahoma Digital, Forensics Professionals, Tulsa, OK, gavin@okdfp.com

Lance Watson
Oklahoma Digital, Forensics Professionals, Tulsa, OK, lance@okdfp.com

David Greer
Center for Information Security, University of Tulsa, Tulsa, OK USA, david-greer@utulsa.edu

Alex Barclay
Center for Information Security, University of Tulsa, Tulsa, OK USA, alex-barclay@utulsa.edu

John Hale
Center for Information Security, University of Tulsa, Tulsa, OK USA, john-hale@utulsa.edu

Scholarly Commons Citation

Manes, Gavin W.; Watson, Lance; Greer, David; Barclay, Alex; and Hale, John, "Towards Redaction of Digital Information from Electronic Devices" (2007). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 1.
https://commons.erau.edu/adfsl/2007/session-12/1

Towards Redaction of Digital Information from Electronic Devices

Gavin W. Manes
Lance Watson
Alex Barclay
David Greer
John Hale

Oklahoma Digital
Forensics Professionals, Inc.
401 S. Boston Ave. Ste. 1701
Tulsa, OK 74103
918-856-5337
gavin@okdfp.com
lance@okdfp.com

Center for Information Security
University of Tulsa
600 S. College Ave.
Tulsa, OK 74104
918-631-3560
gavin-manes@utulsa.edu
alex-barclay@utulsa.edu
david-greer@utulsa.edu
john-hale@utulsa.edu

ABSTRACT

In the discovery portion of court proceedings, it is necessary to produce information to opposing counsel. Traditionally, this information is in paper form with all privileged information removed. Increasingly, the information requested during discovery exists in digital form and savvy counsel is requesting direct access to the original digital source: a broad spectrum of additional digital information can be often be extracted using digital forensics. This paper describes the major problems which must be solved to redact digital information from electronic devices. The primary hurdle facing digital redaction is the lack of a rational process for systematically handling encoded, encrypted, or otherwise complex data objects. Any such process would need to incorporate a method for validating the integrity of electronic or digital redaction processes.

Keywords: digital forensics, redaction, electronic discovery, legal production, privilege

1. INTRODUCTION

Redaction is the process of removing privileged information from a document or set of documents before its presentation to other parties. The reasons for redaction are many and varied [1,7,9,10,11]. This paper will focus on those that apply to the legal community, because the rules of conduct for redaction in the legal system are the most defined and constraining.

During the discovery portion of court proceedings, it is necessary to produce information to opposing counsel. In general, a lawyer's work on a case is protected by the work-product privilege, communications are protected between an attorney and their client, and other parties have no right to this information. The work-product privilege means that any documents prepared in anticipation of litigation or for trial by a party's representative enjoy a qualified immunity from discovery. Other such privileges include: doctor/patient, priest/penitent, and husband/wife. To prove to the court that information is privileged, the party claiming privilege must show that the communication: 1) was made with an expectation of confidentiality, 2) is essential to a socially approved relationship or purpose, and 3) has not been waived by disclosure of the contents of the communications to persons outside of the relationship.

The result of redaction is the production of three pieces of information: an In Camera Copy of the privileged information, a Privilege Log and a Redacted Production Copy of the information. The In Camera copy contains all the items regarded as privileged and is presented to the judge in the case. The Privilege Log and Redacted Production Copy are presented to opposing counsel. If a question arises as to whether a particular item on the privilege log actually meets the burden of privilege, the judge can review the material within the In Camera copy and provide judgment.

Traditionally, the requested information is presented in paper form. Currently, two methods are used to redact paper documents – "blackout" and physical removal. The blackout method involves using a black marker to conceal portions of a document that are considered privileged. The physical removal method involves selecting documents from a group of papers and removing them from the set. Depending on the court's requirements, this may necessitate marking the exact location from which the document was removed.

The same set of concerns exist for privileged information residing on electronic storage devices, but no standard method of digital redaction has been adopted by the legal community. Computerized methods that mimic the blackout process exist, as do those for mimicking the physical removal method [3,5]. The latter typically involves the collection of all readable documents from a computer, placing them in a collection, and selecting the items to redact. Yet, while electronic blackout and removal methods can sanitize a document or set of documents found on an electronic device, they do nothing to redact logical copies or copied fragments of the document that remain.

Moreover, with the introduction of digital forensics and digital evidence into the court system, it is becoming necessary to produce the entire contents of computer disks and other electronic storage devices as evidence. This production goes beyond simply selecting all readable documents on a drive. It involves producing information that exists in free or slack space, deleted items, document fragments and even data that may not be in a readily identifiable format. This collection process produces what is commonly referred to as a forensics copy.

The growing numbers of electronic devices that integrate digital data storage components have exacerbated the issue of redaction. Devices such as cell phones, digital cameras, and digital music players, along with laptops and desktop computers store information using a variety of file systems, media technologies, and data formats. The sheer variety of these storage possibilities differentiates this issue from the traditional methods of redaction and the physical pen-and-paper form they take.

Highlighting this issue is the fact that a single data fragment may be physically replicated multiple times on media. Moreover, simply deleting a file does not usually mean the information is actually erased, but only that the reference point is destroyed. A faithful redaction process for data storage images must account for these subtleties in a systematic and comprehensive manner.

2. DIGITAL REDACTION CHALLENGES

The challenges to digital redaction are numerous and substantial [2,3,6,8]. They include:

- The variety and disparities in electronic storage devices
- The potential for encrypted data
- Files which are deleted but recoverable in slack space or unoccupied regions of a file system
- Data fragmentation
- Isolation of privilege by context for integrated data

To completely redact digital information from an electronic device, it is critical to determine all logical and physical locations of pertinent documents and related data fragments that reside on the digital media. This is because data is routinely stored in multiple locations on most devices. For example, Microsoft Word files are normally saved in a user-selected directory, but may also be automatically backed-up in a temporary folder as a part of normal operation; therefore, a Word document would logically exist at least twice on the computer system.

Similarly, deleting privileged information from digital media does not fully protect it from a well-executed forensic examination. The only versions of a document that can be directly deleted are listed in file mapping tables. Other copies of the item, i.e. those that remain in slack space, might be located during a thorough digital forensic examination.

Determining all of the physical locations of digital information is also important due to the partitioning methods of electronic media and devices. For example, consider the effect of a user creating a file on a LINUX system and subsequently saving it on a FAT partition of the hard drive. The drive is then repartitioned and the file falls out of the new logical partition size, the file is moved into the space on the hard drive reserved for that resized FAT partition. Thus, the file may now exist at least twice on the hard drive; once in the new location and once in its original location.

In determining whether information is privileged, one must be able to interpret the information rationally; if information is unreadable, privilege cannot be determined. This presents a problem on digital devices when information is stored encoded, protected or encrypted. During the redaction process, digital data without rational interpretation may be produced on the grounds that it contains no apparent privilege. The data may actually contain privileged information that is concealed by the encoding. Consequently, if a rational interpretation is later discovered the data can be decoded. This scenario admits the possibility of the privileged information being unknowingly (and unfortunately) revealed to opposing counsel.

Finally, the accuracy of the digital redaction process is extremely important. In producing a redacted copy, care should be taken to demonstrate that the integrity of the redacted copy is preserved as it relates to the source media. The redaction process should only remove the data segments marked for redaction and leave all remaining segments untouched. Thus, digital redaction methods should incorporate validation schemes that offer assurance regarding the integrity of the redaction process.

3. DIGITAL REDACTION COMPONENTS

There are several components required to perform the digital redaction process. The first component is identifying Privileged Information. Next, an Electronic Device Investigation is performed on a Work Copy of an Electronic device. The result of this investigation will identify privileged information, complex and indeterminate data objects and produce an index of redactable items. Finally, the Digital Redaction Process uses Redaction Tokens to produce both a Redacted Production Copy with an associated Privilege Log and an In Camera Copy of the information. The Redacted Production Copy is then re-processed to provide reasonable certainty as to accuracy of the redaction and the In Camera copy is validated through a digital redaction assurance process. These components are unique to the Digital Redaction Process and are detailed below.

3.1 Privileged Information

Electronic redaction allows for the selective exclusion of information protected under privilege as defined by federal, state, and local laws; e.g. attorney-client, doctor-patient, priest-penitent, marital, etc.

The selection of privileged content is based on the current legal standards for such material. These standards involve communication between an accepted member of an accepted privilege class acting in an accepted capacity. Additionally, the court may indicate that certain topics are off-limits and any such related material is to be redacted as well.

3.2 Electronic Device Investigation

The process of redaction typically begins with the creation and/or selection of a Work Copy of an Electronic Device. A Work Copy is typically a forensics copy of the original media, but could be the original media where it is impractical or impossible to create such a copy. A Digital Forensic

Investigation is then performed in order to find all privileged digital information qualifying for redaction, including complex and indeterminate data (described later). This yields an index of redactable items each with a description of their reason for redaction.

3.3 Complex and Indeterminate Data Objects

A digital forensics investigation can yield privileged and non-privileged information. In addition, it may uncover data that is not immediately interpretable. Such data may be structured, compressed or otherwise encoded for interpretation by a special application or method, e.g. an Outlook PST file for an e-mail application. Encryption, data scrambling, or fragmentation may also prevent immediate interpretation of data. Any data that is encoded or structured (and interpretable by a special viewer or application) is treated as a *Complex Data Object*.

A metaphorical example of a Complex Data Object is a piece of used carbon paper: if carbon paper is used multiple times, it may contain interwoven and overlapping documents which cannot be easily interpreted. At this point, it is unclear if the carbon paper contains privileged information; however, analysis could yield the individual documents which may contain privileged information. Clearly it would be irresponsible to produce this carbon paper without performing this analysis and redacting the privileged information.

Complex Data Objects are subject to an additional investigative process using appropriate tools and techniques to interpret the data and make it readable. The interpreted data can then be subject to digital redaction. In cases where no interpretation method is available, such data are labeled *Indeterminate Data Objects*, and may be redacted until a method for interpretation presents itself in the future (and as a result the object is transitioned to a Complex Data Object).

A metaphorical example of an Indeterminate Data Object is again a piece of carbon paper, but one that had been used more extensively. In this case, even if it is not possible to extract individual documents based on current process, it would be irresponsible to produce because a new process could be created at some point in the future to extract the privilege-containing documents.

It should be noted that Complex Data Object Processing is recursive in nature, as these objects may contain other Complex Data Objects. Where no suitable methods are available for interpretation of Complex Data Objects, a degenerate, non-recursive invocation is completed and the object is labeled as indeterminate.

3.4 Digital Redaction

If there are no items to redact, then no privilege or complex/indeterminate items were located and the process is considered complete. Subsequently, the Work Copy used to initialize the current Digital Forensics Investigation and all Privilege Logs associated with that Work Copy are ready for submission to the opposing side. If privileged material is located then Digital Redaction commences.

Using an index of redactable items, portions of the Work Copy are copied to a separate media source and are tagged with identifying location information and a reason for redaction. This becomes the In Camera Copy. In most legal situations, this is the copy of information given to the judge. Concurrently, a Privilege Log is created that contains the identifying information and a reason for redacting for each item.

A Redacted Production Copy is created by copying the Work Copy to a sterile media source using one of a variety of techniques to sanitize or remove each identified portion of the Work Copy based on the index of redactable items. The result of this step is the Redacted Production Copy. This copy should contain no privileged or complex/indeterminate information. Both the Redacted Production Copy and the privilege log are provided to the opposing council.

3.5 Redaction Tokens

Redaction tokens are bit sequences that can be used to replace or stand for private data, complex data objects, or indeterminate data objects in the Redacted Forensic Copy. As such, they provide a method to describe the Redaction process to the court and other examiners. Tokens can help confirm the integrity of the redaction process and provide an accessible layer of abstraction for layperson juries. Implementation requirements will vary depending on legal statutes and precedence, but redaction tokens have inherent advantages which vary based on the method of implementation:

- Tokens create identifiers that bind redacted data objects to the Privilege Log.
- Tokens can act as markers for interoperability with other programs, thus making redacted data segments recognizable to external tools. Forensics suites could recognize markers and skip data carving or sliding window analysis on what is token data/meta-data.
- Tokens can provide a basic audit log, with the token encoding information about the examiner, case, etc.
- Tokens can contain a digital signature of the examiner, providing repudiation and a chain of custody.
- Tokens can include a one-way hash of the redacted object, to verify the integrity of the original object and In Camera copy.
- Tokens can emulate the pre-redaction environment; all data besides the redaction information will appear to be intact.
- Tokens mimic the paper redaction system courts are familiar with, providing an easier conceptual understanding of the processes.

The actual bit sequences for redaction tokens may be generated in a variety of ways, depending on the purpose of the token. The token can serve as a method to represent redacted data, bind meta-information, and provide accountability or any combination thereof. The size of the smallest redacted object might also dictate the potential contents of the token, if the courts want to keep file sizes original. In UTF8, a common encoding format, a name that might be considered privileged could be as small as 6 bytes, thus becoming the maximum token size. On the other hand, redaction of large image files increases the potential size of the token, potentially adding to its abilities.

There are many considerations in generation of the token. Foremost, tokens for each production must be consistent in format, and agreed upon by all parties. Secondly, the token must be amenable to parsing. This issue is more complex than it might initially appear since good tokens must avoid magic numbers and other bit sequences used in file headers and file system constructs. Additionally, tokens should be easily identifiable and be generated in a reasonable amount of time. Lastly, it is vital that a token never reveal information about the contents of the data objects represented in the Redacted Production Copy.

3.6 Reprocessing and Validation

To provide assurance that redaction has been accomplished successfully, the Redacted Production Copy is re-processed through the described redaction process, as many times as necessary to provide reasonable certainty as to accuracy of the redaction. If additional privileged or complex/indeterminate information is found during subsequent examinations, the information is redacted and added to the In Camera Copy and Privilege Log.

Additionally, the In Camera copy is subjected to the post-redaction validation process. This is a separate Electronic Device Investigation; if privilege and complex/indeterminate data rules have been properly applied during the Electronic Device Investigation, every item in the In Camera Copy should be marked for redaction.

4. CONCLUSION AND FUTURE WORK

The increasing use of digital forensics in legal action is an indicator that digital redaction will soon be at the forefront of discussion. Current methods of redaction do not sufficiently address the complexity of the problem in the digital arena. It is only a matter of time before the legal community realizes this and reacts.

Consider an attorney who is using digital forensics to find privileged information from free or slack space. It can be assumed that opposing counsel would never have turned this information over had they known it existed. This slip will give one side an unfair and unwarranted advantage in this case.

Or more ominously, consider an individual engaged in criminal acts fighting a discovery order for digital media by insisting that the computer contains privileged communication between himself and counsel. Since there is no clear path to redact this information, the entire data source must be declared off limits.

Clearly, the time to address digital redaction concerns is now. Future work must identify the best possible methods for digital redaction as they apply to the variety of storage solutions currently available. Because the technologies differ so widely it is assumed that, while the general methodology for each media type will be the same, implementation and execution will vary widely. It seems apparent that the issues inherent in digital redaction are thorny enough to keep research in both the legal and computing communities busy for quite some time.

5. REFERENCES

[1] Anti-Monopoly, Inc. v. Hasbro, Inc., (S.D.N.Y. 1995)

[2] Arkfeld, M. R. (2005), Electronic Discovery and Evidence, Law Partner Publishing, LLC, Phoenix, AZ.

[3] National Security Agency (2006), ‘Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF,’ nsa.gov, 13 December 2005.

[4] National Institute of Standards and Technology (2004), ‘Digital Data Acquisition Tool Specification,’ nist.gov, 4 October 2004.

[5] National Institute of Standards and Technology (2005), ‘Computer Forensics Tool Testing (CFTT),’ cftt.nist.gov, 4 October 2004.

[6] Nichols, R. K., Ryan, D. J., Ryan, Julie J. C. H. (2000), Defending Your Digital Assets, McGraw-Hill, New York.

[7] Northwest Airlines v Local 2000 (D. Minn. 2000).

[8] Palmer G. (2001), ‘A Road Map for Digital Forensic Research,’ the First Digital Forensic Research Workshop (DFRWS), November, Utica, New York.

[9] Playboy Inc. v Welles (S.D. Cal. 1999).

[10] Simon Property Group L.P. v MySimon Inc. (S.D. Ind. 2000).

[11] United States v Alexander (E.D. Mich. 2004).

ABOUT THE AUTHORS

Dr. Gavin W. Manes has both taught and performed hundreds of forensics investigations over the past eight years as a student and a professor at the University of Tulsa. Most recently, he founded Oklahoma Digital Forensics Professionals to fill a gap in the Oklahoma economy by offering digital forensics services. Dr. Manes has a background in computer security, information assurance, telecommunications security, and digital forensics. He was responsible for the creation of the Tulsa Digital Forensics Laboratory on the University of Tulsa campus. As a result, both the Tulsa Police Department Cyber Crimes Unit and the Oklahoma State Bureau of Investigation Computer Crime unit have a permanent presence utilizing the facility.

Lance Watson received his Master of Science in Computer Science from the University of Tulsa in 2003. During his time at TU, he focused on computer and network security, including participation in research regarding telecommunications security. He has earned all five of the federal CNSS/NSTISSI information assurance certifications. Currently, Lance Watson is serving as the Vice President of Client Relations at Oklahoma Digital Forensics Professionals, Inc. Mr. Watson oversees company operations including the collection and analyses of digital devices such as computers, cell phones, and PDAs. Information or evidence found is delivered to clients in easy to read non-technical reports. Mr. Watson's ensures the company adheres to the highest standards of quality, confidentiality, and professionalism.

Alexander Barclay is a Ph.D student at the University of Tulsa in the Enterprise Security Group. His current research interests include risk-adaptive access control, compound exposure analysis, and mach/Darwin security.

David Greer is a Ph.D student at the University of Tulsa at the Center for Information Security. His current research interests include digital forensics, information assurance education, and cyber law. Mr. Greer most recently was the information security specialist at the Oklahoma Department of Career and Technology Education.

Dr. John Hale is an Associate Professor of Computer Science and Director of the Center for Information Security at the University of Tulsa. Dr. Hale has significant expertise in computer security, distributed systems and formal methods. He has published approximately refereed articles and one book, Research Advances in Database and Information Systems Security, Kluwer (2000). Dr. Hale is a member of the IFIP Working Group 11.3 on Database Security and served as Program Co-Chair for its 1999 International Conference. His research sponsored by the NSA and NSF explores the role of operating systems, programming languages and virtual machines in providing secure computation and communication environments.