Security of patient data when decommissioning ultrasound systems

James Moggridge

Ultrasound
2017, Vol. 25(1) 16–24
© The Author(s) 2017
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/1742271X16688043
journals.sagepub.com/home/ult

Abstract

Background: Although ultrasound systems generally archive to Picture Archiving and Communication Systems (PACS), their archiving workflow typically involves storage to an internal hard disk before data are transferred onwards. Deleting records from the local system will delete entries in the database and from the file allocation table or equivalent but, as with a PC, files can be recovered. Great care is taken with disposal of media from a healthcare organisation to prevent data breaches, but ultrasound systems are routinely returned to lease companies, sold on or donated to third parties without such controls.

Methods: In this project, five methods of hard disk erasure were tested on nine ultrasound systems being decommissioned: the system's own delete function; full reinstallation of system software; the manufacturer's own disk wiping service; open source disk wiping software for full and just blank space erasure. Attempts were then made to recover data using open source recovery tools.

Results: All methods deleted patient data as viewable from the ultrasound system and from browsing the disk from a PC. However, patient identifiable data (PID) could be recovered following the system's own deletion and the reinstallation methods. No PID could be recovered after using the manufacturer's wiping service or the open source wiping software.

Conclusion: The typical method of reinstalling an ultrasound system's software may not prevent PID from being recovered. When transferring ownership, care should be taken that an ultrasound system's hard disk has been wiped to a sufficient level, particularly if the scanner is to be returned with approved parts and in a fully working state.

Keywords

Patient data, data security, decommissioning, data protection

Date received: 30 August 2016; accepted: 3 December 2016

Introduction

Most modern ultrasound (US) systems are PC and software driven. Beyond any bespoke hardware, there is almost certain to be a hard disk running a recognisable operating system using files that can be read easily, including files containing patient data. Just as with a PC, tablet or phone, the act of deleting a file may not be sufficient to prevent it being recovered and read again.

The loss of a hard disk from a US system containing patient identifiable data would represent a clear breach of patient confidentiality and would contravene local information governance policies, the Caldicott principles and the Data Protection Act.^{1,2} Healthcare institutions should have allowed pathways for any sharing of patient data that will have been approved by the

local Caldicott guardian. This approval will be on the basis of clinical need to know and patient benefit. Although there may be an approved arrangement to cover offsite repairs of a device or replacement of a data storage component, there will be no such mechanism to cover the return of a system to a lease company or transfer of ownership to any third party. If any patient data exists on such a system, be it readily

Medical Physics Department, University College London Hospitals, London, UK

Corresponding author:

James Moggridge, Medical Physics Department, EGA Wing Level 2, University College London Hospitals, 235 Euston Road, London NW1 2BU, UK.
Email: james.moggridge@uclh.nhs.uk

available or recoverable in some way, the healthcare institution would have no control as to where that data would go, where it would reside and who could access it. That data will survive for the life time of the hard drive, be it within the system or as a scrapped component. Again, this clearly breaks the institution's duty of confidentiality to the patient and contravenes the Data Protection Act.

In addition to demonstrating a failure in the duty of confidentiality between healthcare provider and patient, in recent years loss of data has cost the National Health Service (NHS) more than £500,000.³⁻⁵ Should patient identifiable data be visible to non-approved parties, the responsibility will lie with the healthcare provider where the data originated, regardless of any third parties employed to "dispose" of the hardware containing the data⁵ and regardless of any certification provided as evidence of "safe disposal".

In addition to any financial penalties, the loss or unintended disclosure of patient data can cause significant stress to the patients involved and cause reputational damage to the healthcare entity responsible. Given the media's current appetite for data breach stories,⁶ even the smallest incident involving loss of patient data could have a major impact on a Trust's reputation and cause further anxiety to the patients.

Although US systems are not the only medical devices capable of storing patient data, they represent a unique challenge within the healthcare environment with regard to data control for a number of reasons:

1. They are extremely mobile (compared to other imaging modalities) making it quite easy for disposal to be arranged without notification of any equipment management service.
2. Their widespread use can make it harder to track their lifecycle and it would be quite feasible for a scanner to be purchased, used and disposed of without the local equipment management service being aware.
3. Since they handle imaging data, they are normally provided with a large storage capacity.
4. Imaging data is considerably more standardised than other forms of medical data and, with minimal work, formats such as Digital Imaging and Communications in Medicine (DICOM) are just as easily readable as bitmaps or jpeg files.
5. Due to the complexity of analysis and connectivity requirement, ultrasound scanners are now more likely to be built around a standard operating system rather than be reliant on bespoke operating systems or firmware with unique file formats.

Your local medical device decommissioning process should include steps to ensure that any patient identifiable data is deleted prior to it being taken off site. The

easiest way to achieve this is to remove any data storage component, such as the hard disk and have it destroyed. An ultrasound scanner being decommissioned, however, may be sold on for use elsewhere or have to be returned to a lease company. In either case, the system will need to be in a working condition and compliant with the manufacturer's specifications, which means removal of the hard disk for safe disposal/destruction is not an option, unless you are fortunate to have an identical replacement hard drive which, given the age of most ultrasound systems being decommissioned, seems unlikely. In this case, the only option might be to rely on the system's own software to delete any stored patient studies. However, data recovery from corrupt or damaged media is a widely available service and there are many open source products online that can recover files that have been deleted. The same principles can be applied to any PC-based medical devices.

The aim of this project was to investigate whether open source software could be used to analyse and recover data from an ultrasound system hard disk and what methods could be used to securely wipe a hard disk before it was deemed safe to dispose of.

The software used

For file recovery

TestDisk. TestDisk⁷ (version 7.0 C. Grenier, CGI Security, Le Perreux sur Marne, France) is open source file recovery software designed for recovery of deleted or damaged file partition tables. Its functionality has expanded to include an application called PhotoRec which can be pointed to a hard disk partition and set to look for certain file types (including DICOM) that have been deleted. It is an extremely useful application and is included on most file recovery and forensic distributions such as Live Rescue CD and Caine.

For file deletion

DBAN. DBAN^{8,9} (version 2.3.0, Blancco Technology Group Headquarters, Georgia, USA) stands for "Darik's Boot and Nuke". It is open source software that securely erases data on a hard disk drive (HDD) by overwriting with pseudorandom numbers. It can overwrite according to a number of recognised protocols, e.g. Department of Defence (DoD) 5220.22-M (3 or 7 pass) protocol.

For medical file examination

Weasis. Weasis¹⁰ (version 2.0.4, N. Roduit) is open source, multi-purpose web-based DICOM viewing software.

ImageJ. ImageJ¹¹ (version 1.48v, W. Rashband, National Institutes of Health, USA) is open source software for image analysis that can read DICOM files but requires an additional Bio-Formats plugin¹² for reading compressed files.

Notepad or your preferred text editor. DICOM meta-data is generally stored as plain text, meaning any standard text editing software can be used to open a DICOM file and view available fields. The operating system might complain but the header data can be viewed.

Bleachbit. Bleachbit¹³ (version 1.12, A. Ziem, USA) is open source software that can be used to wipe only blank space on a hard disk – this may be useful in a situation where you have used the US system's own software to delete entries and images from the archive and want to make sure they are securely wiped while keeping the system software intact.

What level of wiping is sufficient?

Hard disk wiping software, including DBAN, will refer to a wiping level and number of passes. It is now generally agreed that due to changes in hard disk track density, for any hard drive made after 2001 that is over 15 GB in size (i.e. nearly all modern ultrasound systems), only a single pass is required to both clean and purge the media.¹⁴ This was investigated during testing and a single wipe pass proved as effective as 3 or 7 when using Test Disk/PhotoRec to attempt recovery of the files and the single wipe process was considerably faster. Please refer to your Information Governance (IG) team though to find out what your own local policy is.

Methods

Preliminary disk inspection

A disk containing patient study information was extracted from one of the ultrasound systems, connected to a personal computer (PC) via Integrated Drive Electronics (IDE) to a Universal Serial Bus (USB) converter, and the partition, folder and file structure was examined to determine what the nature of the files might be and where patient data might reside so that these areas could be targeted in the later recovery methods.

The deletion methods tested

Five different deletion methods were tested, on nine ultrasound systems due for decommissioning, to determine an effective means of ensuring that patient data was truly deleted from an ultrasound system.

Method 1. In Method 1, data were deleted from the ultrasound system using the system's own operating software, meaning both database entries and files associated with the patient should be deleted.

A single scanner from the nine was selected as a sample to see if any files could be recovered following such deletion. A test examination was stored on the ultrasound scanner and the patient details noted before being deleted. The hard disk was then extracted, connected to the PC and TestDisk/PhotoRec was run on the partition with the patient archive to determine what files could be recovered. From the recovered files, attempts were made to locate the one study that had been created prior to deletion of the data. From the number of recovered files, it was clear that deleting via the ultrasound system's own data management tools was not sufficient, so a decision was made to move on to testing full software reinstallation as a deletion method (Method 2).

Method 2. In Method 2, data were deleted via a full reinstall of the scanner operating software, including formatting of all hard disk partitions – this is effectively reformatting the hard disk, and any operating system or user partitions should be removed and then rebuilt as new.

Following the checks from Method 1, all nine US systems had a full software reinstall which should completely erase and rebuild the HDD (this could be considered the standard approach to removal of patient data from a US system) and is probably the method used by the ultrasound scanner maintenance provider if asked to clear the system of all user data. After the reinstallation, each scanner was started up to confirm that it was operational and that the archive was empty of data. After this, all nine scanners had their hard disks extracted and each HDD was connected to a PC via an IDE to USB converter and TestDisk/PhotoRec was used to try and recover any files still present on the rebuilt archive partition.

Method 3. Method 3 involved data deletion via a hard disk wipe using DBAN software. Eight HDDs were then wiped using DBAN (Department of Defence 3 pass method) and TestDisk/PhotoRec was run on the HDDs again and results recorded. Hard disks were then returned to their respective systems where the software was reinstalled and correct operation was confirmed.

Method 4. Method 4 was a certified deletion via a Falcon Forensics device supplied and run by a third party support provider. One HDD was wiped using a Falcon Forensics device supplied by GE Healthcare and TestDisk/PhotoRec was run. The hard disk was

refitted into its respective US system before the system and application software were reinstalled and normal operation was confirmed.

Method 5. Method 5 consisted of deletion of examination data using the ultrasound system's own operating software and then cleaning any blank space left on the HDD using BleachBit.

Examinations were stored on a system. The HDD was extracted from the system and connected to an IDE to USB converter. The disk was examined to demonstrate that the examination files could be found and read using ImageJ, Weasis, Notepad and picture management software. The hard disk was then reinserted into the ultrasound system and then once started up, the examination data were deleted from the archive using the scanner's own data management tools as with Method 1. The HDD was then extracted from the scanner again and reconnected to the PC via USB and TestDisk/PhotoRec was then used to test if any files could be recovered. Blank space wiping software, BleachBit, was then run on each partition before the disk was re-examined with TestDisk/PhotoRec to see which files could be recovered. Finally, the disk was reinserted into the ultrasound system to confirm that the scanner could start up normally again.

Rationale behind the deletion method used

Methods 1–3 could be seen to represent the expected best efforts of the person performing the deletion process moving from clinician to a level that would need to be specifically requested and quoted for by the external service provider or the original equipment manufacturer (OEM).

The first is likely to be the method employed by an end user charged with preparing a system ready to be taken off site or sold on. Typically, just the patient entries stored in the patient database, along with any patient files, will be deleted from the system and any information referencing the clinic and/or hospital would be removed. This level of deletion would require just knowledge of how to use the system archive tools, which a day-to-day user of the equipment should be familiar with.

The second method is likely to be employed if the maintenance provider for the system is asked just to clear the system of user data. Reloading the software is often the quickest and most thorough way to achieve this. Typically, this will reinstall the operating system on the hard drive from a clean image and, provided the right options are selected, will also rebuild any user partitions that would contain data relating to the site and any patient studies. The resulting system should

have its software running as new, that is, clean of any user entries including hospital information, site-specific presets, connectivity settings and any patient information or study-related files.

The third method could be employed by the ultrasound physics, scientific computing or medical equipment management team. It does make the assumption that the person performing the wipe knows enough about the system to locate and remove the hard drive and also reinstall the software once the disk has been wiped or that the support provider could reinstall the software post wipe.

The fourth method is likely to be used if you have hired a third party or requested a secure forensic level wipe from the ultrasound support provider. As with methods 2 and 3, the system software would need to be reinstalled once the wipe has been performed.

Method 5 perhaps represents the ideal approach – theoretically, if used in conjunction with Method 1; any patient data should be effectively wiped whilst leaving the system and application software intact.

Results

File structure of ultrasound scanner pre-deletion

Examination of a HDD from one of the systems indicated that the hard drive was divided into three partitions: System, User and Restore. Out of these, it was apparent that the user partition contained the examination database and examination images. Examination folders contained three types of file per image stored (Figure 1):

1. A file with no extension which could be opened as a DICOM image using ImageJ;
2. A jpg file with the same name as 1;
3. A jpg file with the same name as 1 and 2 but with the extension “index.jpg”.

Each of these named files was the same image but in different formats. The entire folder structure could be imported using Weasis with each examination listed as a separate DICOM study.

Results for Method 1

Following Method 1, the disk was analysed; the results are shown in Table 1. Although the original plan was to search for a specific test patient that had been added to the system prior to the process, data relating to this patient could not be located due to the vast number of patient files recovered (see Table 1) and the corrupted nature of the DICOM files, which meant they

Figure 1. Folder structure and file format from system's patient archive, pre-deletion.

could not be searched through automatically for patient identifiers. To check whether the recovered files were readable and contained patient data, three readily available programs were used to access them: Microsoft Paint for jpeg and bitmap files; ImageJ and Weasis for DICOM files; and Notepad for attempted reading of the DICOM headers. A more detailed description of the recovered files and typical contents can be found later in the section entitled “The nature of the recovered files”.

Results for Method 2

Following Method 2, the disks were analysed and the files recovered are summarised in Table 1. As with Method 1, recovered files were analysed using: Microsoft Paint for jpeg and bitmap files; ImageJ and Weasis for DICOM files; Notepad for attempted reading of the DICOM headers. Files displayed the same characteristics and quantity of patient identifiable data as demonstrated from Method 1 (see Figure 2(a) and (b)).

Results for Method 3

Following on from disk wiping with DBAN, no files could be recovered from any hard drive. Results are shown in Table 1.

Results for Method 4

Following on from use of the Forensic Falcon device, no data could be recovered from the HDD. Results are shown in Table 1.

Results for Method 5

As expected from the results for Method 1, after using the ultrasound system's own disk management tools to delete data, DICOM and jpg files could still be recovered. However, following use of BleachBit to clean the blank space, no examination files could be recovered (Table 2). Upon being reinserted into the ultrasound system, the scanner started up normally.

The nature of the recovered files

Due to the large number of recovered files from methods 1 and 2, it was not possible to examine them all, so random samples of both jpg and DICOM files were selected. Files were analysed using: Microsoft Paint for jpeg and bitmap files; ImageJ, Weasis and Microsoft Notepad for DICOM files.

The sample of recovered jpeg files selected could all be opened with Paint. A typical file is shown in Figure 2(a). Please note that patient name, date of birth, ID and information about the

Table 1. The numbers of files of different types recovered following deletions processes 1, 2, 3 and 4.

	DCM (number of files recovered post Method 2)	JPEG (number of files recovered post Method 2)	BMP (number of files recovered post Method 2)	Number of files recovered post Method 3
Scanner 1 (Method 1)	48,853 ^a	93,235 ^a	27 ^a	N/A
Scanner 1	48,853	93,235	27	0
Scanner 2	48,076	90,835	137	0
Scanner 3	37,345	72,488	28	0
Scanner 4	25,577	49,689	372	0
Scanner 5	29,009	55,992	2	0
Scanner 6	6973	12,364	113	0
Scanner 7	42,679	84,269	1	0
Scanner 8	43,777	83,938	13	0
Scanner 9 (Method 4)	39,181	75,390	0	0 ^b

^aPost Method 1.^bPost Method 4.

DCM: Data Constrained Modelling; JPEG: Joint Photographic Experts Group; BMP: Bitmap; N/A: Not Applicable.

clinic/hospital were all visible. There were some files that were distorted and could not be read but the majority had legible patient-related information imprinted on them.

The majority of recovered DICOM files were corrupt and not recognisable by any DICOM file reading software; they could only be read consistently with a text editor where it seemed only the header was present. Attempts to open them with DICOM software failed, with a file info error relating to incorrect size. It could be that, given the age of the systems and number of files recovered, deleted DICOM files had been partially written over and hence were missing image information. This hypothesis is supported by the fact that the recovered DICOM files from the testing in Method 5, which were freshly deleted with no further studies stored on the system, were nearly all readable.

Opening the recovered DICOM files in Notepad or other text editor enabled the DICOM header to be read as shown in Figure 2(b). It is interesting to note that upon examination of the original folder structure from the HDDs, the DICOM files did not have a file extension. However, the recovered files had a “.dcm” suffix suggesting the recovery software identified the file type correctly even if the contents were corrupt.

Discussion

Standard means of deleting patient data from an ultrasound scanner's own operating software can give the impression that patient data has been wiped from the internal hard disk, but the data likely to be recoverable.

As was shown from the results, files can be restored using readily available recovery software and patient identifiable information is viewable from both recovered image files and any DICOM files. Although the DICOM files were corrupted, the metadata relating to the patient could still be read with a standard text editor. Taking such systems off site would represent a breach of patient confidentiality and the Data Protection Act. From past cases such as the NHS Surrey incident,⁵ it is unlikely that claiming data were deleted from the system would be an adequate defence. It would be necessary to demonstrate that attempts to read data from the hard drive following these measures were unsuccessful and that the data were truly wiped. With this in mind, it is vital that as part of the decommissioning process, there is a protocol in place where either the existing hard disk is removed and destroyed, with a replacement installed, or measures are taken to ensure that hard disk contents are completely wiped via third party software.

Physical destruction of the hard drive is normally the safest way of ensuring that data cannot be recovered.

Figure 2. (a) A typical jpeg file recovered following software reload. Please note that the red boxes hide genuine readily accessible patient and clinic information. (b) An extract from a recovered DICOM file that should have been deleted. This has been opened using notepad. Please note the full set of patient and clinic information visible as clear text.

However, this is not always an option if the system has to be returned to a leasing company in a working state or the plan is to sell it on as a working system. It may be that you can purchase a replacement hard drive as an approved spare part, but at the point of decommissioning, the system is likely to be using a hard drive that is

no longer readily available. Perhaps each system decommissioning could be considered on a case-by-case basis and include a form of cost analysis to determine the best approach to data destruction.

Some centres are now adding the inclusion of wiping of data by the supplier upon decommissioning to the

Table 2. The numbers of files of different types recovered using Method 5 pre and post wipe.

File type	Pre delete from system using system software	Recovered from system following delete using system software	Number of files recovered post BleachBit
Index.jpg	224	516	0
.jpg	224		
No extensions (assumed dcm)	224	237	0

terms and conditions of any new ultrasound system procurement to avoid additional fees. Using the service provider could also avoid the need to reinstall the system software, which can be an arduous if not impossible task. Pushing responsibility onto the suppliers of the ultrasound equipment may force manufacturers into introducing their own measures to ensure your data is safe; for example, most operating systems now offer a means of encrypting the hard disk and thus protecting data. Adding such options to a PC-driven ultrasound system would not represent a huge leap in technology and should, arguably, become the industry standard, particularly for point of care equipment.

If ultrasound systems employ a more bespoke file format rather than plain DICOM or jpeg, file recovery may be hindered, but not impossible, particularly if there are any send buffers on the system that contain more conventional file formats. There are other companies that can offer a data wiping service, including various second-hand medical device suppliers that, as well as offering to purchase used ultrasound equipment, will also offer to ensure that all data are removed first.

Whichever data wiping option is selected, remember that, regardless of any certification provided, it is the healthcare establishment that will be held accountable should any of its data leak into the public domain. With this in mind:

- If you perform the wiping process:
 - Check that it has worked as expected and no recoverable files remain.
- If using a third party:
 - Make sure that they tell you what their processes are (including security during transport) so you can validate and risk assess them yourself.
 - Ask if they can return a sample to you for testing following their destruction process.
 - Request a site visit to check the system and processes to ensure that your media are handled responsibly and processes are adhered to.

Wiping without removing the system software

As demonstrated from Method 5, there is disk cleaning software available that will only wipe over the blank sectors of a hard disk, i.e. files still present will be left intact but any remnants of past writes from deleted files will be wiped. Such a technique can allow an end user to effectively clean the hard disk of any patient data whilst keeping the operating system and device software in a working condition.

Such a solution does rely though on the end user being able to delete all patient data from the system prior to running the wiping software. The end user also needs to be aware that there may be send queues, spoolers or buffers located in other parts of the drive that may still remain after deleting patients from the scanner's archive. Such folders and files will have to be deleted from the disk directly and there would always be a risk that some patient identifiable files would be missed.

Perhaps the better solution would be a hybrid approach whereby a full software installation is performed to return the system to an "as new" state before the blank space cleaning software is run to ensure that no files can be recovered.

Conclusion

Deleting records from an ultrasound scanner may delete database entries but files can still be recovered. Even more robust methods of resetting a system of patient data, such as full software reloads, will not be sufficient to wipe all patient data files from a hard disk. Software reloads will often just reformat the hard disk and rebuild any patient data directory structures from a saved disk image. In doing this, the files will still be recoverable and the partition table on the disk will be as before. It may be cost effective to arrange with the manufacturers prior to purchase, for them upon decommissioning, to take responsibility for the hard disk being cleaned or replaced.

It is important for medical physics or engineering departments to develop a protocol for dealing with disk wiping upon decommissioning of hard drive-equipped medical equipment. Remember that the onus for patient data protection is on the institute that recorded that data and the device or its components may have a life after it passes on from your hospital. This might be especially true for systems brought in for test or demonstration purposes.

Contributorship

JM researched, carried out the study, performed the analysis and wrote the paper.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethical approval

Not applicable

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Guarantor

JM

References

1. The Caldicott Committee *Report on the review of patient-identifiable information*. London: The Department of Health, 1997.
2. *The Data Protection Act (1998)*. London: The Stationary Office, <http://www.legislation.gov.uk/ukpga/1998/29/contents> (1998, accessed 11 December 2016).
3. Rossi B. *NHS Trust faces £350k fine following hard disk theft*. Information Age, <http://www.information-age.com/nhs-trust-faces-350k-fine-following-hard-disk-theft-1684088/> (2012, accessed 11 December 2016).
4. Savage M. NHS 'loses' thousands of medical records. *The Independent*, 24 May 2009, <http://www.independent.co.uk/news/uk/politics/nhs-loses-thousands-of-medical-records-1690398.html> (2009, accessed 13 December 2016).
5. Ashford W. ICO issues £200,000 penalty for failed IT disposal. *Computer Weekly*, 12 July 2013, <http://www.computerweekly.com/news/2240187927/ICO-issues-200000-penalty-for-failed-IT-disposal> (2013, accessed 11 December 2016).
6. Borland S. 2,000 NHS patients' records are lost every day with more than two million serious data breaches logged since the start of 2011. *The Daily Mail Online*, 15 February 2014, <http://www.dailymail.co.uk/news/article-2559876/2-000-NHS-patients-records-lost-day-two-million-data-breaches-logged-start-2011.html#ixzz4Si8wAti0> (2014, accessed 11 December 2016).
7. Grenier C. *PhotoRec, DataRecovery*, <http://www.cgsecurity.org/wiki/PhotoRec%20> (2015, accessed 11 December 2016).
8. Wikipedia, *Darik's Boot and Nuke*, Wikipedia, https://en.wikipedia.org/wiki/Darik%27s_Boot_and_Nuke (2016, accessed 13 December 2016).
9. DBAN. *Data Wiping Software*, <http://www.dban.org> (accessed 13 December 2016).
10. Weasis. *Portable DICOM Viewer*, <https://dcm4che.atlassian.net/wiki/display/WEA/Home> (accessed 13 December 2016).
11. Rashband W. *ImageJ – Image processing and analysis in Java*, <https://imagej.nih.gov/ij/> (accessed 13 December 2016).
12. LOCI, *Bio-Formats plugin for reading compressed DICOM images*, <http://www.loci.wisc.edu/ome/formats.html> (accessed 13 December 2016).
13. Ziam A. *BleachBit*, <https://www.bleachbit.org> (accessed 13 December 2016).
14. Pieters-Michaud N. *Debunking the 3-pass overwrite requirement*. IT Asset Requirement: Value Creation through disposition, http://cascadeam.typepad.com/it_asset_retirement_value/2012/10/debunking-the-3-pass-overwrite-requirement.html (2012, accessed 13 December 2016).