Evidence Destruction

This lesson will focus on how digital evidence should be disposed of after the retention period has expired. It is crucial that evidence is securely destroyed, luckily there are a number of methods we can use to achieve this. We will cover:

- Degaussing
- File Shredding
- Physical Shredding
- Hydraulic Crusher
- Overwriting

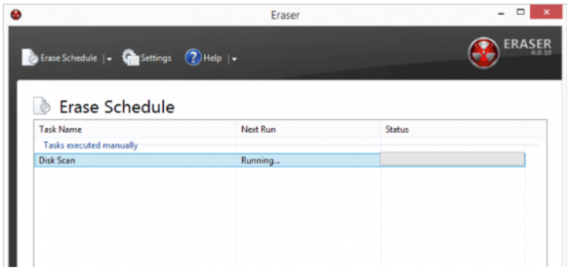
DEGAUSSING

When exposed to the powerful magnetic field of a degausser, the magnetic data on a tape or hard disk is neutralized or erased. Degaussing is the guaranteed form of hard drive erasure, which means that it serves as the standard method of data destruction. Using the right degausser will guarantee that your information is no longer retrievable.

FILE SHREDDING

File Shredding can sometimes be the same as manually deleting a file or folder, and as we covered at the start of the course, these files can be recovered unless they are overwritten. This is **not** a secure method of deleting digital evidence, as there is the possibility it can be recovered. However, some file shredding programs utilize different methods to overwrite or sanitize the data that has been selected for shredding. One method that is known as the DoD 5220.22-M Wipe Method includes 3 steps:

- **Pass 1**: Writes a zero and verifies the write.
- **Pass 2**: Writes a one and verifies the write.
- **Pass 3**: Writes a random character and verifies the write.



Erase Schedule

Task Name	Next Run	Status
Tasks executed manually		
Disk Scan	Running...	

PHYSICAL SHREDDING

Physical shredding is the process of destroying physical storage media so that it can't be reassembled and accessed. A hard drive, USB, or other hardware will be shredded into small pieces using industrial-grade destruction equipment. The hard drive shredding process destroys the drive platters, mechanisms, and the electronic components rendering the data unrecoverable.

HYDRAULIC CRUSHER

The name says it all, this method of destruction uses a hydraulic press with a metal rod that is pushed straight through the hard drive. Punching a hole with approximately 3,400 kilos of force pressure completely destroys the drive platters, rippling and fracturing the magnetic surfaces and rendering the drive data unrecoverable. Other methods can include bending the hard drives until they snap, as shown in the image below.

OVERWRITING

Organizations may want to reuse hard drives or USBs that have been involved in forensic investigations, so overwriting may be the best option as it doesn't result in physical destruction. As covered at the start of this domain, data is typically still accessible until it has been overwritten. We can simply write zeros to a hard drive, overwriting any existing data. Windows offers a function called Diskpart that allows you to completely clear a hard drive from the command prompt.

< Previous Topic
Mark Complete ✓

Back to Lesson