Acquisition of a fake RAID using GRUB

Widely accepted acquisition methods for RAID systems include forensic imaging of an assembled RAID volume (a virtual drive) and forensic imaging of individual drives in a RAID (images of these drives can be assembled on a forensic workstation later).

Forensic imaging of an assembled RAID volume is straightforward for hardware RAID configurations, because a RAID controller is exposing an assembled virtual drive for an operating system, thus there is no need to use an additional RAID driver during the acquisition.

When a software RAID configuration (no RAID controller is present, all RAID management is performed by an operating system) is encountered, an acquisition tool can be used to image individual drives. If an operating system used during the acquisition (like a forensic Live USB distribution) supports a particular software RAID setup (e.g. includes a specific RAID driver), it is feasible to image an assembled virtual drive instead of individual physical drives.

Fake RAID configurations are usually treated as software RAID ones, because an operating system is required to have a RAID driver in order to start (assemble) the array after the early boot sequence.

Forensic imaging of an assembled RAID volume allows easy access to file systems stored inside the array, but an examiner can miss data stored on RAID drives, but not used by the array. Also, a RAID controller can modify data stored on drives during the acquisition (e.g. by updating internal metadata structures used for managing the array).

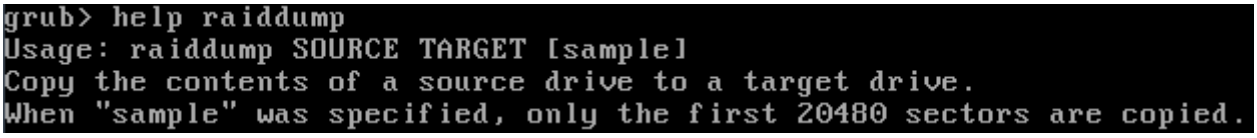
Forensic imaging of individual drives is more solid. However, in order to gain access to file systems and other types of data stored inside, an examiner has to assemble (rebuild) the array. If a RAID metadata structure is known to and supported by a tool used to rebuild the array, the assembly process is easy. If no RAID metadata structures were used to create the array, or their format is unknown, an examiner can try to guess the unknown parameters (like a stripe size, an order of drives, etc.) of the array, typically this process involves assembling the array step-by-step using all reasonable values of the parameters until the assembled volume contains partitions and/or file systems that look valid. When dealing with full disk encryption, the process of guessing the unknown RAID parameters will likely fail, because there is no way to tell whether or not blocks of encrypted data have the correct order (without trying to decrypt the data).

Taking advantage of a fake RAID

While an operating system installed on a hardware RAID volume can boot with no problem, because there is no need for a special driver, an operating system installed on a software RAID volume requires a boot loader supporting this RAID implementation in order to boot, thus proprietary operating systems have problems with third-party software RAID configurations. A fake RAID attempts to solve this problem by allowing the boot loader to load the kernel of an operating system and the RAID driver without bothering about the RAID. This is achieved by a fake RAID controller intercepting the 0x13 BIOS interrupt used by a boot loader to read data from a disk, assembling the array, and giving assembled data back to the boot loader for each read request, so the boot loader is unaware of the RAID, treating all RAID drives as a single disk (containing assembled data). When no fake RAID controller is used, similar operations can be performed by a BIOS itself. Since modern operating systems do not use the 0x13 BIOS interrupt to interact with drives after the early boot sequence (this is slow and limited), a special RAID driver is still required.

Forensic examiners can use the 0x13 BIOS interrupt to read assembled data from a fake RAID on a suspect computer, if other means of assembling the array failed. An examiner can acquire a forensic image of a whole assembled virtual disk this way; moreover, a small sample of assembled data can be acquired quickly in order to produce enough information to rebuild the array using images of individual drives acquired before.

So, even in 2016 a drive with DOS can be useful during forensic acquisitions. However, DOS is out-of-date, so a GRUB module was written to perform simple disk-to-disk acquisitions using the 0x13 BIOS interrupt (https://github.com/msuhanov/grub-raiddump).



It should be noted that the same method can be utilized to perform acquisitions of a fake RAID on UEFI systems, if EFI services provide read access to the assembled volume.