**Question 1:** Look up at least one criminal case that involved data carving. Was the technique useful for the prosecution or for the defence?

**Answer:** The case I have chosen is that of an International Child Abuse Case which was solved by Croatian police. The case revolved around child pornography and its storage within the suspects computer, memory dumps and hard drive images.

The Croatian Authorities were able to use a piece of software called Belkasoft Evidence Center was used to solve the case. Five different PC’s were seized as part of the instigation, all of which were processed using the software. The software was able to successfully un cover quite a substantial amount of evidence that would later be used it court.

The software itself can allow a user to perform a full thorough text search across many files. It can automatically locate, process and analyse evidence stored in RAM, find encrypted files, carve Internet chat logs, Web browsing history and email communications including attachments such as digital pictures and videos.

The software is even capable of recovering data that has been deleted by the user. Through a technique called data carving, the software is able to re assemble files from raw data fragments with no file system metadata available. This means that even though an individual may think they are safe deleting a file, they are by any means no way safe at all.

It is clear that the prosecution benefited more from this technique than the defence. The prosecution team were able to use hard forensic evidence to convict the suspect(s) of 13 cases of “Exploitation of children for pornography” and one case of “Unauthorized use of personal data”. The defence had nothing to nullify the evidence and therefore came out the worse of the two.

**Question 2:** Download and review Gramm-Leach-Bliley, HIPAA, and Sarbanes-Oxley. Each of these pieces of legislation have some commonalities and some major differences. What are the main commonly shared features, and how do they significantly differ?

**Answer:** All three of these acts were passed into law to either enhance or grant protection to an individual or group of individuals. They all revolve around the idea of data, its uses and penalties associated with misconducts.

Gramm–Leach–Bliley Act: This act deals with the protection, disclosure, storage of a customer’s financial data / information. It is mainly used in the financial services industry, which includes banking, insurance, and investment institutions. This act ensures that all customers data is fully protected and that breaches of it will be followed with severe punishments.

Health Insurance Portability and Accountability Act: This act deals with the standards of health insurance coverage and the privacy of health-related data / information. The act deals solely with the administrative, physical, and technical safeguards for health information stored in an electronic format. This act ensures that all patients data is fully protected and that breaches of it will be followed with severe punishments.

Sarbanes–Oxley Act: This act deals with the reliability of financial reporting by public companies and their accounting firms. Private companies are not directly subject to the act; however, standards have been increased over financial reporting in general which indirectly affects them. This act ensures that all financial data is fully correct and to date. Because of this, people like investors or board members can always be sure that their investments are financially sound and that they are complying with all relevant legal acts.

Although these acts protect an individual / set of individuals in one way or another, they all do so in different industries and in different ways.