Q1:
Case Number511-02-11/1-V-K-9/14 GN/IKC,Bjelovar, 23.04.2014

In this case data carving was extremely useful for the prosecution, without it, prosecution of the following suspect would have been difficult if not impossible without recovering the deleted evidence.
Police in Croatia using a data carving tool named Belkasoft Evidence Center were able to gather large quantities of data from 5 computers using Memory Dumps and Hard Drive images. Much of this data had been deleted, the uncovered evidence which was mostly comprised of Web History, Social Media usage was then used to further assist the investigation of the suspect and some was also used in court as evidence of his guilt.

Evidence of criminal exploitation performed by perpetrators was also discovered on the PC's and forwarded on to the relevant criminal associations.

State of Western Australia versus Buchanan (2009)

In this scenario data carving ended up being not of use to either the prosecution or the defendant due to poor data forensics techniques and presentation of evidence. The presumption of innocence was mostly ignored and a number of questionable conclusions based on faulty reasoning were made. Digital evidence was also provided without appropriate context, timelines and documentation to the court which lead to the prosecution failing.

BTK Killer Case

In this scenario digital forensics helped with the discovery and subsequent prosecution of the BTK serial killer Dennis Rader, who had evaded capture for 2 decades. It was discovered through data carving of a digital tape he had sent to taunt the police, although the disk had been wiped. Data Forensic specialists were able to recover document

metadata from the disk which indicated that it had been used by someone called Dennis at a local Church. A quick google search then confirmed his identity and he was arrested.
This was then subsequently used in trial as a part of the evidence against him.

James Kent:

In this case, a prolific child pornographer was discovered and prosecuted through evidence gained through data carving. James Kent was a professor at Marist College NYC when he recieved an upgrade to his old computer. What he did not realise is that all his old files including deleted ones were transferred across to the new device. Which meant when he was having issues months later with his device and the IT department ran a virus scan the administrator discovered a lot of old files with .jpg in the unallocated space. When they confirmed the content of these files the harddrive was handed over to the authorities. Subsequently hundreds of files and pieces of meta data were found in his mozilla and Internet explorer cache files.

Q2:

Commonalities Between the 3 Pieces of Legislation:

- GLBA & HIPAA both cover how to Secure, protect and maintain confidentiality of person's private information
- All 3 legislations leave the implementation of the secure controls of data up to the company themselves and do not mandate specific technological solutions.
- GLBA & HIPAA both require that an organization provide a clear privacy statement for users/customers.
- All 3 mandate IT Controls which maintain security, accountability, integrity and privacy of the data.

Differences Between 3 Legislations:

- Industry covered, HIPAA Covers Healthcare industry, Sox covers the accounting practices of firms and GLBA covers insurance companies and other financial institutions.
- Sox hardly mentions IT at all in the legislation however has a huge impact on IT practices.
- Sox has a particular focus on strong document retention and auditability controls. Which ensure no data is deleted.