WHAT DIGITAL EVIDENCE ARE YOU MISSING IN COMMERCIAL CRASHES?

BY: Trish McGarvey, Digital Forensics Specialist – Columbus, OH

Trish McGarvey is a Digital Forensics Expert for STARS Consulting, LLC. We utilize cutting edge technologies to combine digital forensics, crash reconstruction, and drones in our investigations to garner critical evidence.

Digital Forensic Examiners and Accident Reconstruction Investigators are similar, but they investigate an incident from different perspectives. Crash reconstruction determines what happened in the seconds prior to and during a crash. In other words, a "snapshot" is obtained. A digital forensic examiner determines what happened before, during, and after the crash. Collectively, the two provide a more complete "picture" of the event.

Commercial motor vehicle (CMV) technologies are growing exponentially and as a result– so is the data that can be collected – which can be invaluable to a case. This article will cover the different types of data that can be acquired from CMV's, their drivers, and the companies they work for—and a few of the ways the drivers/companies may attempt to hide this data.

What types of data can be acquired from the vehicles?

With today's current technologies, vehicles—including CMV's—are ultimately computers with wheels. There is an abundance of information that can be extracted from the truck—if you know where to look—and how to obtain the data.

The following is a brief overview of what may be available from a CMV:

- Black Boxes – Electronic Control Modules (ECM's), which contain crash and setting data helpful in crash investigation. However, proprietary software that is used for ECM reports can be used to alter and delete data.
- Telematic Systems – send data – HOS, GPS location, time, speed, engine parameters, hard-stop/lane departure incidents, and may be transmitted via satellite or cellular communications. Can be easily hacked.
- Crash Avoidance Systems
- DDEC Assurance
- Bendix – ESP full stability control system & Wingman Fusion
- WABCO – ESCsmart & OnGuard MAX
- VORAD – (Vehicle Onboard Radar) analysis of speeds, deceleration and trajectory of all vehicles
- Electronic Logging Devices (ELD's) – potential to alter/delete data by using "ghost drivers" and/or amending entries

There may be valuable data that can be extracted from passenger vehicles involved in truck crashes. Infotainment & Telematic Forensics can recover:

- Devices/Call/Text logs
- Hard braking/acceleration
- GPS data – routes & speed
- Velocity logs
- System information – lights on/off, gear position, doors open/closed

What can be obtained from or about the drivers?

The driver more than likely will possess personal, as well as work-related mobile devices. This may include cell phones, iPads, computers, GPS units, dashcams, and/or fitness devices to name a few.

Mobile devices have evolved significantly over the last few years. Today, cell phones are tantamount to small computers that capture virtually every moment of our lives. The data contained on these devices have been compared to a personal diary that includes: pictures, videos, private documents, secure financial information, and even more importantly—our routines, patterns, and everyday habits. In other words, if data is recovered from a mobile device, it often paints a very personal, and potentially embarrassing portrait of the individual. The data—or lack of data that can be acquired from these devices may be crucial to a case and answer a multitude of questions:

- Was the driver on the phone or texting at the time of the incident?
- Was the driver on social media, another app, or the web?
- Did the driver use wiping software to delete data?
- Had the driver been searching the web for ways to bypass or disable security features on the tractor/trailer or how to hack ELD's?
- Was the device locked or unlocked?
- Is there GPS data that may show the speed or stops made?

A driver may attempt to hide calls and/or texts by utilizing apps such as WhatsApp, Viber, TextFree, to list a few. These types of apps use WiFi instead of cellular networks, therefore, the data will not be displayed on cell records. TextFree even provides the user with another phone number to utilize. Best practice is to acquire and analyze the cell phone, as well as obtain the cell records to verify data. There are also apps that will attempt to conceal data - steganography. There are additional apps that the drivers/companies may use in an attempt to wipe (delete) data from the device in an effort to conceal evidence.

We have handled cases where law enforcement analyzed a phone and said there was no usage during the incident, only to uncover the device was actually being manipulated using some of the abovementioned techniques. In one such case, the agency reported no usage. Later,

however, we determined the driver was actually watching a pornographic video while driving down the highway prior to the crash. Needless to say, this case settled quickly. It is paramount to be aware of what apps are available, what techniques may be used, and how to uncover critical information.

Additionally, GPS units, dashcams, fitness devices, and any other mobile devices should also be analyzed for relative data. An easily overlooked type of media is SD cards. SD card data may be altered or deleted by a driver/company, but it is relatively easy to recover deleted data from these cards. Even if mobile devices have been damaged, ChipOff technology can be utilized to obtain data directly from the chip-level.

What can be obtained from the companies?

There can be a vast amount of digital data that can be collected from the systems in a company's office. This data includes:

- Dispatch units - client information, broker information, Telematic system data between the driver and the office
- HR systems – driver file, training records, personnel file, compliance management
- Maintenance record systems – service, repair and inspection history on tractors and trailers, crash records

Companies may attempt to tamper with data. The information should always be verified by checking the original data.

Conclusion:

New technologies and applications are introduced so frequently that thorough investigation and inquiry is required to successfully determine data sources, as well as, data integrity in heavy truck crashes. Spoliation/Preservation letters should be sent immediately.