

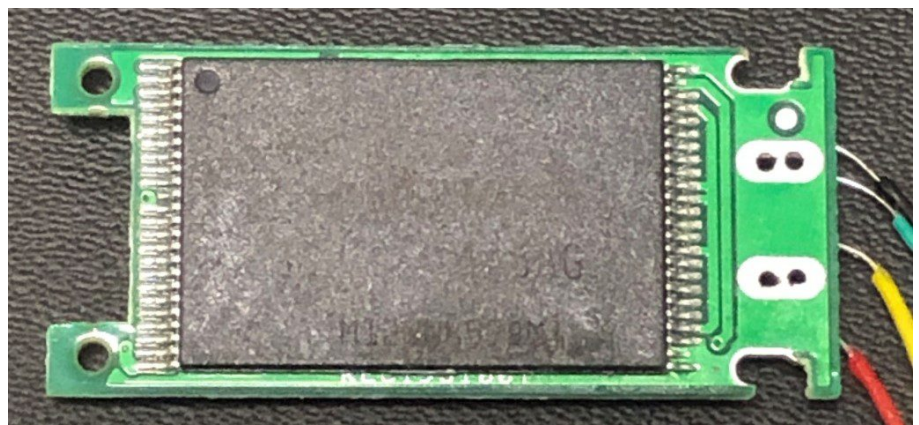
## Carpe Datum "Seize the Data"

Timothy R. Primrose, Mobile Forensic Analyst

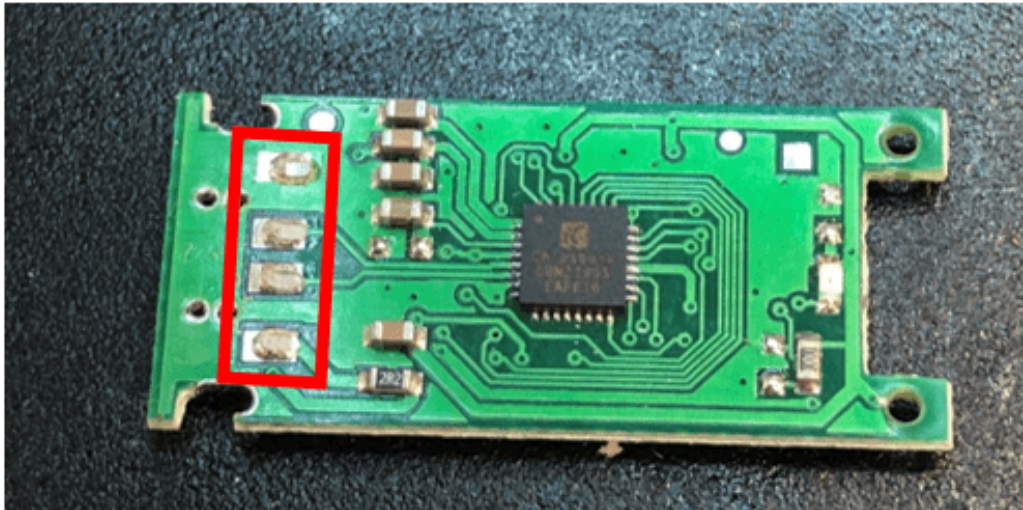
In the field of digital forensics, it's important for investigators to collect data in a forensically sound manner. This means collecting data without manipulating or deleting any data. Not every device that we receive is functioning or in its manufactured state. Cell phones are crushed in car accidents, SD cards are thrown in washing machines, and thumb drives are stepped on. In these scenarios, data can still be retrieved. Cell phones can be repaired and SD cards can be properly dried, while any built-up corrosion can be cleaned. If someone tries to destroy evidence by stepping on a thumb drive, the location of where the data is stored will most likely remain intact.



The portion of a thumb drive that we see is just a protective shell for a logic board that contains the chip that data is stored on. Stepping on a thumb drive will disrupt the connections established for communication between the logic board and a computer. The chip location is adhered to the underside of the logic board.

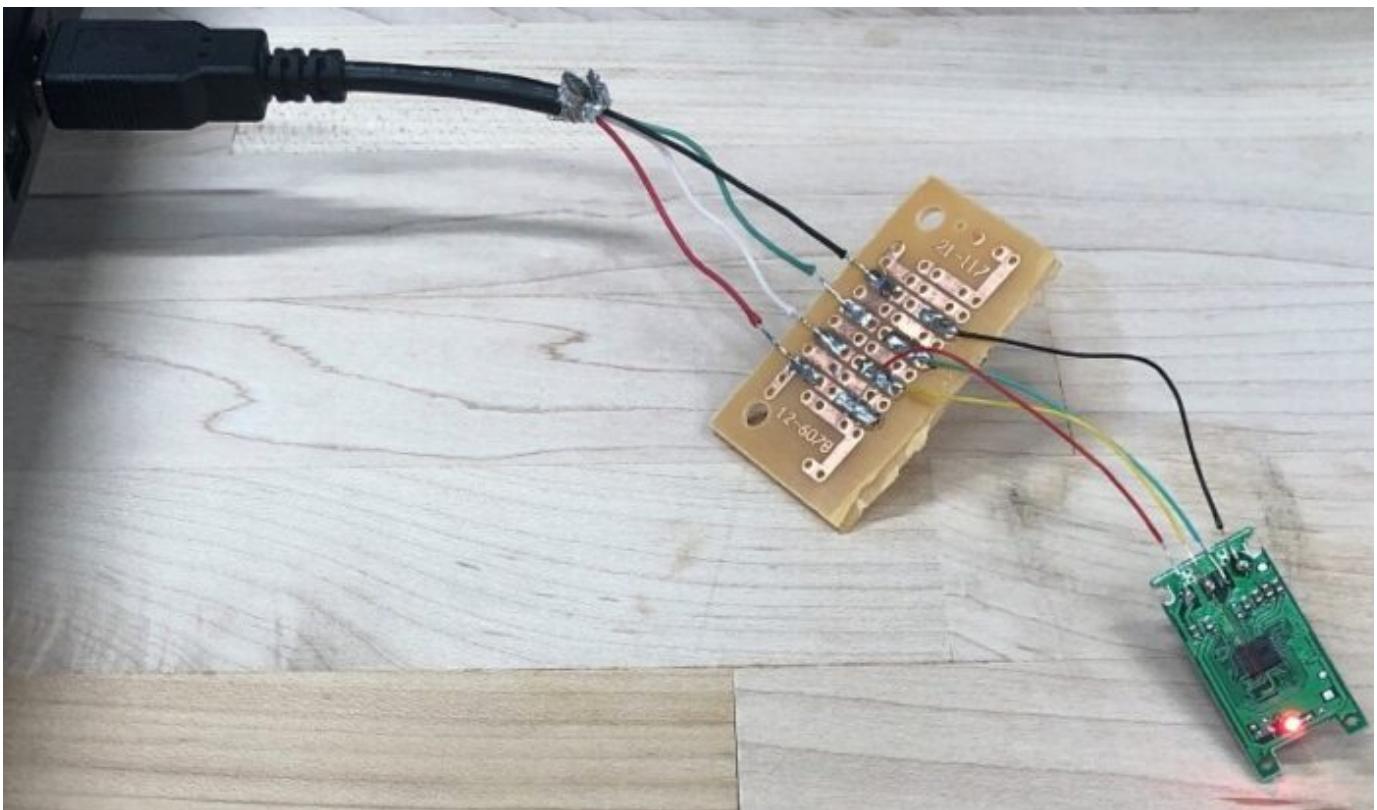


Although the connection is lost, the data is not gone, it still resides on the chip. There are four pads on the logic board that are connected to the USB connector in order to communicate with a computer or other supported devices. The four pads have different roles. Two of the pads are used to provide power to the device. The remaining two pads control data in (data being stored) and data out (data being accessed or removed). The four pads are indicated below.



USB  
Connector

There are four pins on the end of the USB connector that are typically adhered to these four pads in order to transfer data to and from the device. Since this device was smashed and the logic board remained intact, we were able to solder wires to the pads and wire this logic board to an existing USB cable. Solder is a metal alloy that melts at high temperatures and cools quickly to hold electrical components in place.



After I soldered the wires, we were able to connect the “thumb drive” to a computer and access the data stored on it. To verify that this worked, check out the red light in the bottom right-hand corner of the image, this shows that the device had power.

The goal for digital forensic investigators is to seize the data. This could mean fixing a device or finding a work around as illustrated in this scenario. As long as the process is conducted in a forensically sound manner, the data can be seized properly and securely, making it admissible in court.

***Timothy R. Primrose, Mobile Forensics Analyst with DJS Associates, Inc., can be reached via email at [experts@forensicDJS.com](mailto:experts@forensicDJS.com) or via phone at 215-659-2010.***