Tracy Harvey Module 9 Group Dropbox

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**What standards must evidence meet in order to be considered admissible in a court of law, when this evidence is collected from a suspect's computer?**

There are a lot of things that need to be considered for evidence to be admissible in court. Was the evidence obtained legally such as with a search warrant, does it pertain to the case, was it tampered with, chain of custody and so on.

**Explain what "chain of custody" means.**

It is a document that tracks where and when the evidence was accessed and by whom, to prove that the evidence has not been outside a secure environment unless it was being handled by an authorized official.

**What, if any, tools exist for gathering data that is highly volatile, such as the data that is stored in RAM, if the belief exists that this data might lead to a conviction?**

One tool is Magnet RAM capture, this tool is designed to capture the contents of a computer’s physical memory. Other software is Volatility Framework which is an open source program for memory forensics mostly used to analyze RAM dumps and WinPmem which is a tool to create RAM dumps on windows machines.

**What would be the implication of** **continuing an investigation, using digital forensic tools, once evidence of "child pornography" was uncovered, without being a duly appointed representative of law enforcement nor an official representative of the Department of Justice (DoJ)?**

As with all evidence that is collected you need to be an authorized representative that has a legal right to be collecting any evidence, regardless of what you find “child pornography” or not. If you were not a legal representative authorized to be doing these searches then the evidence that you collect could possibly be thrown out as an illegal search at best. At worst you as the investigator might be charged with a crime due to you not having any right to be sifting through someone’s personal data.