

# [Quiz 1](https://assignbuster.com/quiz-1/)

[Law](https://assignbuster.com/essay-subjects/law/)

CCJS421 – Quiz Match each of the following terms with the picture it best matches (use each term and picture only once):
a. Thumb drive
b. Hard disk drive
c. Workstation
d. Server
e. Mobile device
f. Small Computer System Interface (SCSI)
g. Serial attached SCSI
h. Serial ATA (SATA) (Type A)
i. External SATA (eSATA)
j. Universal Serial Bus (USB)
k. Firewire 400
l. Firewire 800
m. Zero insertion force (ZIF)
Universal Serial Bus (USB)
Mobile Devise
External SATA (eSATA)
Thumb Drive
Workstation
Zero insertion force (ZIF)
Firewire 800
Serial ATA (SATA) (Type A)
Small Computer System Interface (SCSI)
Firewire 400
Hard disk drive
\_ Server
Serial attached SCSI
2. Match the following terms with its associated definition:
a. Forensic soundness (or forensically sound)
b. Malware
c. Hash value
d. Forensic suite
e. Tool belt approach
f. Evidence custody (or property custody) document
g. Verification
h. Bit-stream copy (or forensic image)
i. Repeatability
Malware A general term used to describe a program or piece of code that is general harmful to the normal use or operation of a computer system.
Forensic suite The general phrase used to describe collections of digital forensic tools or single tools that enable multiple analyses of digital evidence; examples include Guidance Software’s Encase Forensic and Technology Pathway’s ProDiscover Basic.
Bit-stream copy (or forensic image) a bit-by-bit duplicate of data on the original or source medium, created via a process called “ acquisition” or “ imaging.”
Repeatability\_ a concept used to describe the ability to get the same results each time from the same test or examination directed at the same data set or piece of evidence.
Evidence custody (or property custody) document A printed form indicating who has signed out and been in physical possession of evidence. Many agencies also use this form to provide a physical description of evidence for later identification.
Tool belt approach a concept used to describe a varied approach to a digital forensic examination, whereby multiple hardware or software solutions are chosen (regardless of brand name) because they are best suited to a particular task.
Harsh value A process used to determine that a forensic image is an exact, bit-by-bit copy of the original source media.
Verification an expression (often composed of hexadecimal values) derived from the application of a specific mathematical algorithm to a particular set of data, which can be used to verify data integrity or identify specific files.
Forensic soundness(or forensically sound)\_ A general term used to describe placing an emphasis on documenting, processing, and analyzing digital evidence (in the context of computer crime and security) in such a way as to preserve its usefulness in any potential litigation or criminal investigation.
3. Data recovery involves recovering information from a computer , that was deleted by mistake or lost during a power surge or server crash, for example.
a. Data recovery c. Computer forensics
b. Network forensics d. Disaster recovery
4. The basic plan for your investigation includes gathering the evidence, establishing the \_ nature of the case and performing the forensic analysis.
a. risk assessment c. chain of custody
b. nature of the case d. location of the evidence
5. To conduct your investigation and analysis, you must have a specially configured personal computer (PC) known as a forensic workstations\_\_\_\_.
a. mobile workstation c. forensic lab
b. forensic workstation d. recovery workstation
Reference
Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Burlington: Elsevier Science.