CCDC Inject

INJECT NAME	Legality of Log Files
INJECT ID	LEGP05A

INJECT DESCRIPTION:
Your organization typically does not have firewall logging enabled. During a suspected breach by malware, the IT Director asked you to enable logging on all the rules within the firewall security policy for a 24 hour period. Subsequently you were asked to prepare a log file extract by editing out all the traffic except that associated with 4 particularly external IP addresses.

The corporate attorneys have asked you to testify in court with regard to the log file since the opposing side is challenge the evidence under the hearsay rules.

Do you have any concerns with regards to the file you prepared being admitted into evidence ?

INJECT DELIVERABLE
Prepare a clearly written business memo that recaps what the hearsay issue is with regard to digital log files. Enumerate view of the admissibility of the log files as evidence given the context of the hearsay issue.