WGU C702 - Forensics and Network Intrusion Exam

1. **Which documentation should a forensic examiner prepare prior to a dynamic analysis** **>>>>**The full path and location of the file being investigated

2. **What allows for a lawful search to be conducted without a warrant or probable cause** **>>>>**Consent of person with authority

3. **A forensic investigator is tasked with retrieving evidence where the primary server has been erased.The investigator needs to rely on network logs and backup tapes to base their conclusions on while testifying in court. Which information found in rules of evidence, Rule 1001, helps determine if this testimony is acceptable to the court** **>>>>**Definition of original evidence

4. **When can a forensic investigator collect evidence without formal consent** **>>>>**When properly worded banners are displayed on the computer screen

5. **Who determines whether a forensic investigation should take place if a**

situation is undocumented in the standard operating procedures >>>>Decisionmaker

6. **Which situation leads to a civil investigation** >>>>Disputes between two partiesthat relate to a contract violation

7. **Which rule does a forensic investigator need to follow** >>>>Use well-knownstandard procedures

8. **What is the focus of Locard's exchange principle** >>>>Anyone entering a crimescene takes something with them and leaves something behind.

9. **What is the focus of the enterprise theory of investigation (ETI)** >>>>Solvingone crime can tie it back to a criminal organization's activities.

10. **A forensic investigator is searching a Windows XP computer image for information about a deleted Word document. The investigator already viewed the sixth file that was deleted from the computer. Two additional files were deleted. What is the name of the last file the investigator opens**

>>>>$R7.doc

11. **What is a benefit of a web application firewall (WAF)** >>>>Acts as a reverseproxy to inspect all HTTP traffic

12. **How does a hacker bypass a web application firewall (WAF) with the toggle case technique** >>>>By randomly capitalizing some of the characters

13. **During a recent scan of a network, a network administrator sent ICMP echo 8 packets to each IP address being used in the network.The ICMP echo 8 packets contained an invalid media access control (MAC) address. Logs showed that one device replied with ICMP echo 0 packets. What does the reply from the single device indicate** >>>>The machine is in promiscuous mode.