Perform Incident Response and Session Recording

The first steps taken by an investigator when an incident has occurred constitute the incident response. The following rules should be followed during the incident response phase of an investigation:

- The router should not be rebooted unless absolutely necessary, according to the rules of router forensics. If the router is rebooted, valuable information can be lost.
- All information and evidence acquired must be recorded.
- No modifications should be made to the information and evidence acquired.

Figure 4-2  Chain of custody forms document the evidence-gathering phase of an investigation.