BAOU Education for All

List of Practical

Practical-1	List all the important sections that should be included in the investigation report.
Practical-2	List some popular tools used for packet sniffing.
Practical-3	Write steps for data acquisition process
Practical-4	What are the steps for preparing first responder's toolkit.
Practical-5	Give examples of some common digital evidences.
Practical-6	List steps for digital evidence investigation process
Practical-7	Explain the booting process of Window 7 in detail.
Practical-8	State the usage and forensic importance of PsLoggedon, Netsessions, logonsessions tools.
Practical-9	How the deleted and lost files are recovered in a windows system?
Practical-10	How is registry information important in windows forensics?
Practical-11	List Tools for passwords cracking
Practical-12	How are the network logs captured and analysed?
Practical-13	List Major tasks an investigator needs to do while

	performing web application forensics
Practical-14	Describe any 3 web application forensic tools
Practical-15	Describe the structure of SMTP messaging with a neat diagram
Practical-16	Which headers in SMTP useful in tracing a message sender identity?
Practical-17	List and describe atleast 4 email attacks
Practical-18	List major sources of evidences in a mobile device
Practical-19	Steps for mobile forensic process
Practical-20	What are the different mobile device logs important during mobile acquisition?
Practical-21	Write the steps involved in mobile acquisition.
Practical-22	Describe the various steps of report preparation in detail.
Practical-23	Describe the process of data encapsulation.
Practical-24	How to protect your sensitive resources?
Practical-25	State and define different wireless Hacking Methodology
Practical-26	What are the best practices on using wireless networks?
Practical-27	Explain different tools in intrusion detection.
Practical-28	Write down few points to prevent your network from anonymous attack
Practical-29	List out key features and types of Hardware

	Security Module (HSM)
Practical-30	Explain Working of Vulnerability Assessment Tool
Practical-31	Write steps of Penetration Testing Method
Practical-32	How can we defend against Social Engineering
Practical-33	Draw and discuss the social engineering life cycle. Ans.
Practical-34	Explain the Cyber security Incident Chain
Practical-35	Write Cyber Security Incident Checklist
Practical-36	Explain Five Phases of Cyber Security Incident Management
Practical-37	What to do When a Cyber Security Incident Occurs and You Are not Prepared
Practical-38	Write your key recommendations for handling incidents
Practical-39	List major steps that should be performed when a technical professional believes that a serious incident has occurred and the organization does not have an incident response capability available
Practical-40	What information should be provided when reporting an incident?