(Slide-2) Hardware tools:

1. Hardware-based Keyloggers:

Keyllama: A USB hardware keylogger that records keystrokes from a computer keyboard. It can be connected between the computer and the keyboard to capture and store keystrokes.

KeyGrabber USB Keylogger: Another USB keylogger that records keystrokes from a keyboard and stores the data in its internal memory.

PS/2 Keylogger: A keylogger designed to intercept keystrokes from a computer's PS/2 keyboard connector.

2. Network Packet Capture Devices:

Pcapng: A portable network packet capture device that allows capturing and analyzing network traffic for forensic analysis.

Wireshark: Although primarily a software-based packet capture tool, Wireshark can also be used in combination with supported hardware devices to capture network packets effectively.

Network TAPs: Hardware devices that are placed between network devices to passively monitor and capture network traffic without interfering with network operation.

3. Mobile Forensic Kits:

Cellebrite UFED (Universal Forensic Extraction Device): A popular mobile forensic kit used by law enforcement and digital forensics professionals to extract data from various mobile devices.

MSAB XRY: Another mobile forensic solution that supports data extraction and analysis from a wide range of mobile devices.

Oxygen Forensic Detective: A comprehensive mobile forensic kit that supports data extraction from smartphones, tablets, GPS devices, and other mobile devices.