Tools and Methods used in Cyber Crime

Proxy Server

- It is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.
- Proxies were invented to add structure and encapsulation to distributed systems.
- Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing anonymity

Anonymizer

- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.
- It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information

Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a genuine (legal) organization to ensnare individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Keylogger

- Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Spyware is largely invisible software that gathers information about your computer use, including browsing. Key loggers are a form of

spyware that capture every keystroke you type; they can send this information to remote servers, where log-in information--including your passwords--can be extracted and used.

- A keylogger is a tool that captures and records a user's keystrokes. It can record instant messages, email, passwords and any other information you type at any time using your keyboard. Keyloggers can be hardware or software.
- Spyware is any software that installs itself on your computer and starts covertly monitoring your online behaviour without your knowledge or permission. Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties.

There are two common types of keyloggers.

Software and Hardware keyloggers.

- Software Keyloggers.
- Hardware Keyloggers.
- Spear Phishing.
- Drive-by-Downloads.
- Trojan Horse.
- 2-Step Verification.
- Install Anti Malware Software
- Use Key Encryption Software

Hardware Keyloggers

- Hardware keyloggers are small hardware devices.
- These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Software Keyloggers

Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Software

keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user.

Antikeylogger

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.
- Advantages of using antikeylogger are as follows:
- Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
- This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs if not updated, it does not serve the purpose, which makes the users at risk.

Spywares

Spyware is a type of malware, that is installed on computers which collects information about users without their knowledge. The presence of Spyware is typically hidden, from the user, it is secretly installed on the user's personal computer. Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.