Sniffing and Scrapping:

	Sniffing	Scrapping
Definition	Passive interception of data from network traffic.	Automated extraction of data from web pages.
Purpose	Analysing network communication.	Gathering information from websites.
Data Source	Network packets, often unencrypted.	HTML content of web pages.
Legal Concerns	Can raise privacy and security issues.	Legality depends on website's Terms of Service.
Permissions	Generally requires no direct consent.	Often violates website's ToS if done without consent.
Tools	Wireshark, tcpdump, network analyzers,	Web scraping libraries/ frameworks (BeautifulSoup, etc.)
Complexity	Requires technical networking knowledge.	Requires web development knowledge.
Real-time	Can monitor data as it's being transmitted.	Extracts static data; doesn't monitor in real-time.
Frequency	Can capture data constantly in a network.	Typically performed periodically or on demand.
Use Case	Network troubleshooting, security analysis.	Price comparison, content aggregation, research.
Challenges	Encryption can hinder data capture.	Website structure changes can break scraping.
Ethics	Can be invasive if used maliciously.	Respect robots.txt and terms of websites.