1) Explain the process of Jailbreaking or Rooting a smartphone. Which security mechanism should be deactivated?

   1) Exploit code-execution vulnerability to deploy and execute jailbreak-payload.

   2) Execute payload, if required gain root by exploiting privilege escalation vulnerability.

   3) Patch LLB, iBoot and Kernel to remove signature checks.

   4) Install cydia to allow installation of unsigned 3rd party applications.

   It will deactivated Sandboxing, Memory protection, Code signing and Encryption.

2) Why we need Smartphone Forensics ? In the story of FBI vs Apple; i) why Apple couldn't decrypt the data of the phone? ii) how a backdoor compromises the security of smartphone?

   Because Since the use of small portable devices has become widespread, the probability of a digital device being involved in a criminal action is growing significantly bigger. And a digital device can participate in a crime by different means. So we need mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.

3) Why Android smartphone are affected more by malwares?

   Because Android system is open source. And also, Google Play as a centralized point of distribution not provides users with confidence that the apps they download have been tested and validated by Google.

4) Why we need intelligent cyber security mechanisms to protect modern smartphones? Why existing security mechanisms are not 'though'?

   First because discovers previously unknown patterns and knowledge. Second, high-value predictions that can guide better decisions and smart actions in real time without human intervention. Also, quickly and automatically produce models that can analyze bigger, more complex data and deliver faster, more accurate results.

   Our current existing security mechanisms are not though enough because we have much more threats than protections.

	Antivirus	Encryption	Firewall	PIN/Password
Mobile service fraud				✓
Social Engineering Attacks				✓
Privacy exposure				✓
DoS service			✓	
Malwares	✓			
Lost/stolen				✓
Insider		✓		✓

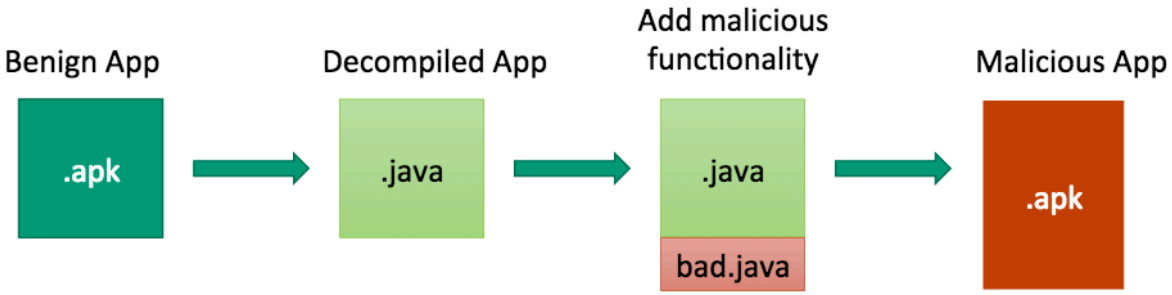
5) How artificial intelligent and machine learning will change our everyday life? Give an example related to cyber security?

Because recently, more data is generated in everywhere, AI is the study of how to create intelligent agents. In practice, it is how to program a computer to behave and perform a task as an intelligent agent would. And Machine Learning relates with the study, design and development of the algorithms that give computers the capability to learn without being explicitly programmed. These will help us deal with huge amount of information much more efficiently.

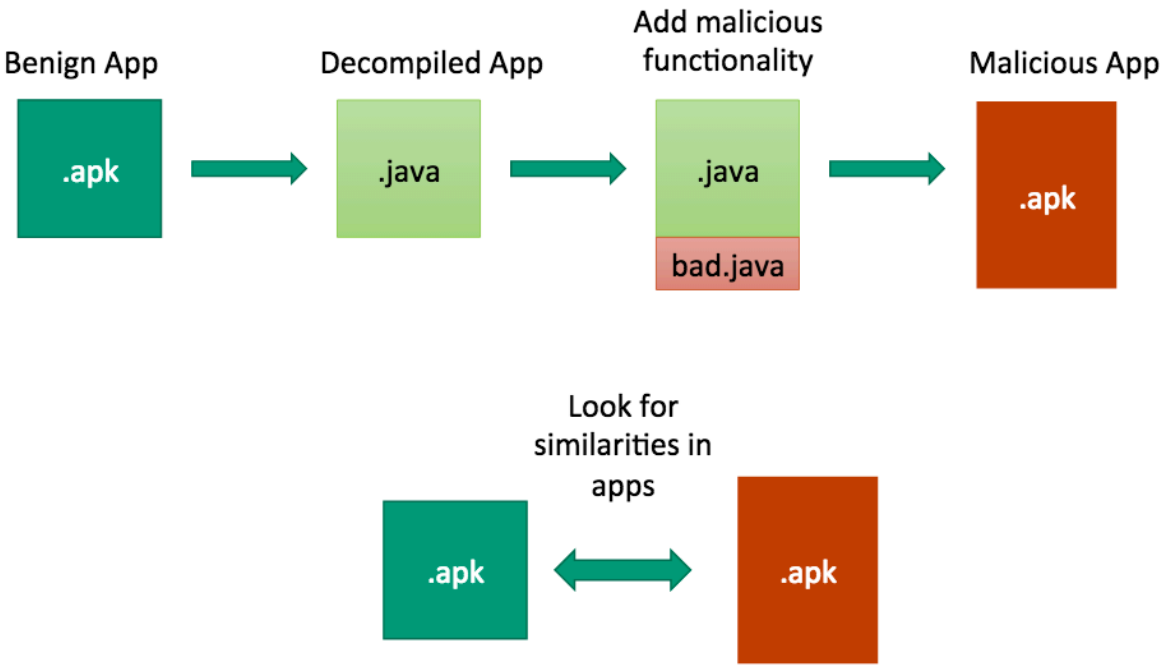
We can use machine learning technologies like Artificial neural networks or Decision Trees to solve information security problems, such as Malware detection, Intrusion detection or SPAM mitigation etc.

6) Explain the method of App repackaging aiming to create an Android malware

Repackaging Android apps



Detecting repackaged apps



Detecting similarities, decompile and compare code, extract control-flow graph, collect called APIs, compare requested permissions and apply reverse engineering techniques