Capturing Traffic

Contents

- Networking for Capturing traffic
- ARP Cache Poisoning
- SSL Man-in-the-Middle Attacks

1. Networking for Capturing traffic

- **Hubs Device**:
  - Layer one device of the OSI model.
  - Send frames out on all ports including the port in which the frame was received on

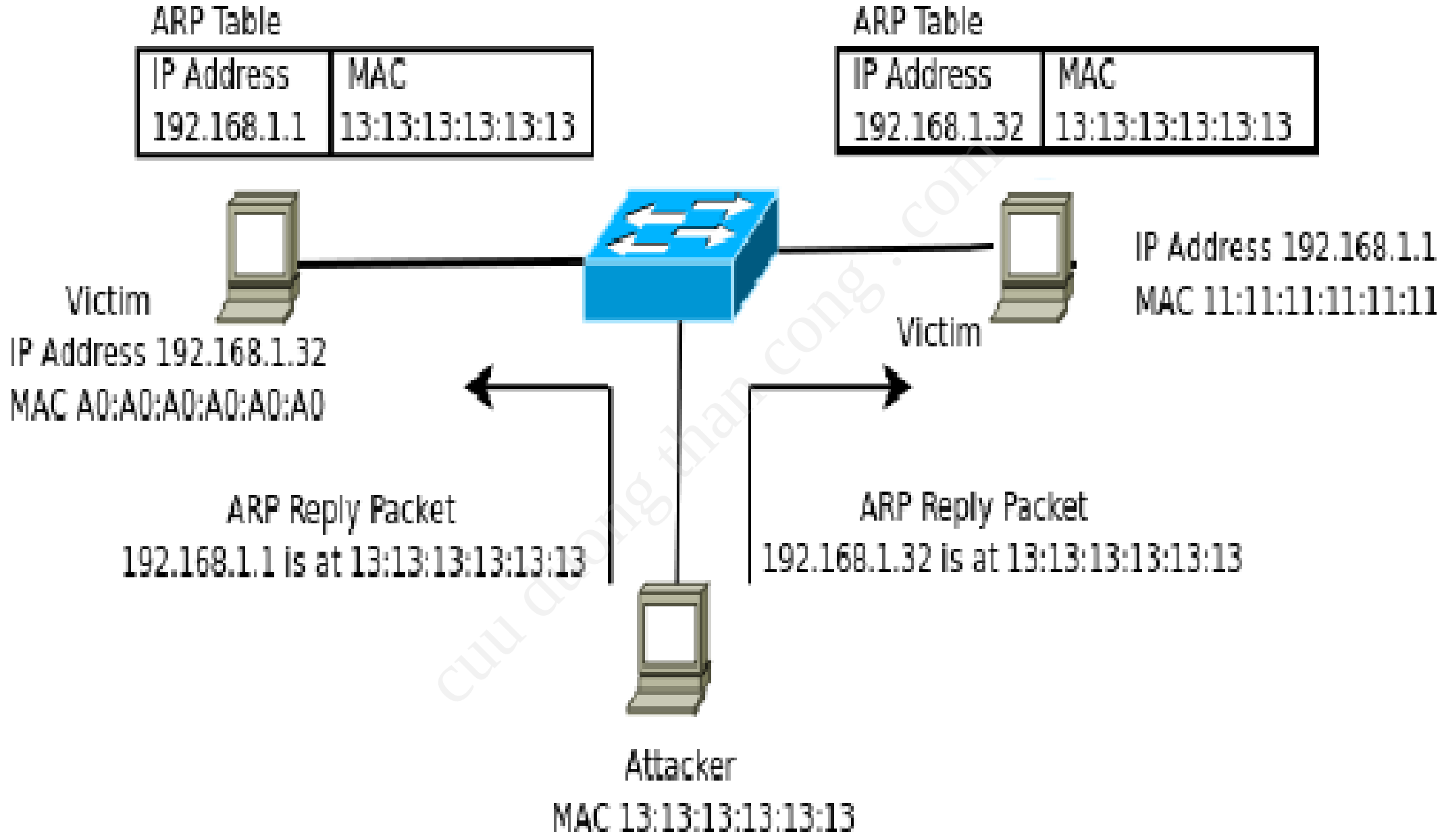
- Switches Device:
  - MAC address table
  - Switches provide separate collision domains on each port

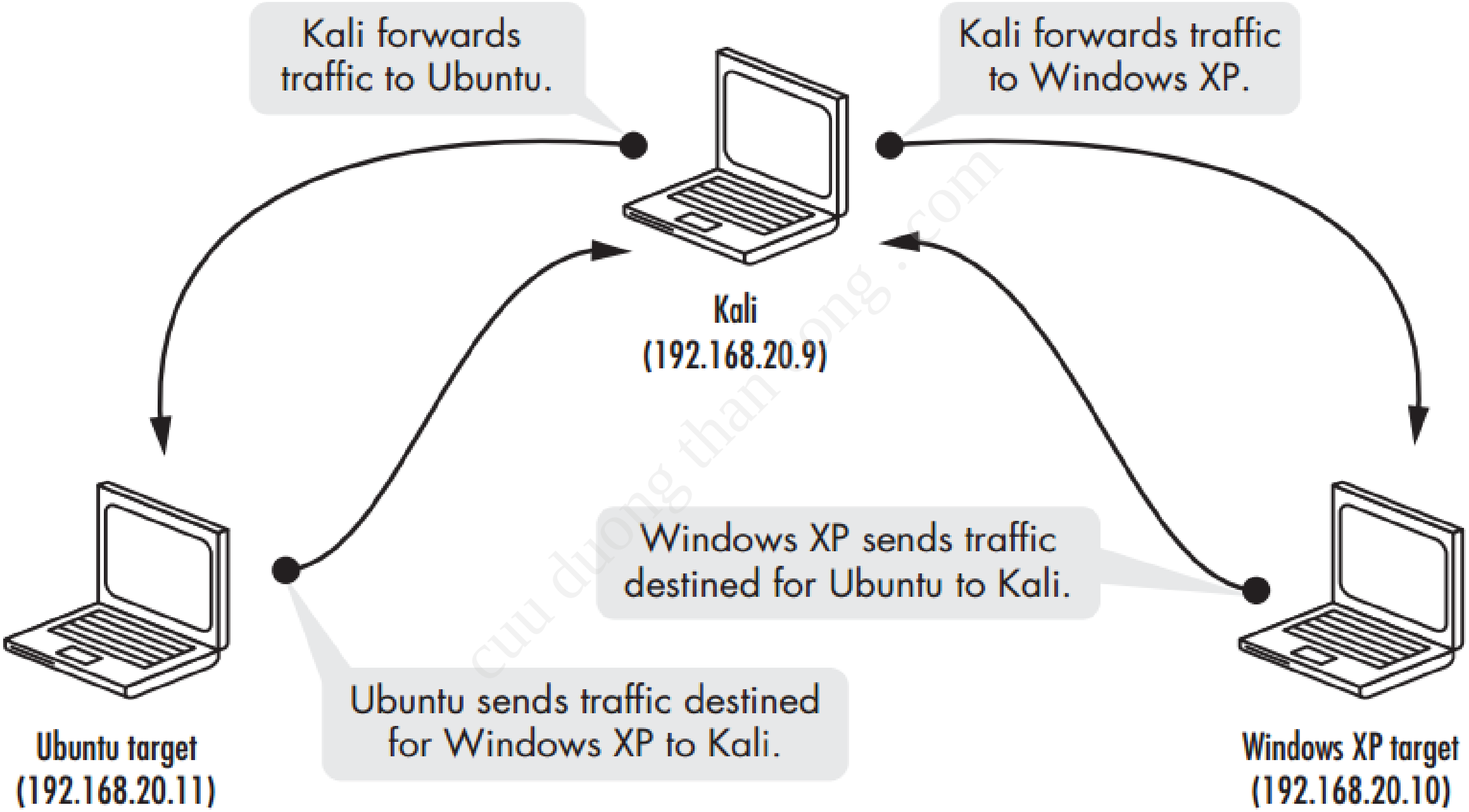
Using Wireshark

- Wireshark is a graphical network protocol analyzer that lets us take a deep dive into the individual packets moving around the network.
- Wireshark can be used to capture Ethernet, wireless, Bluetooth, and many other kinds of traffic

2. ARP Cache Poisoning

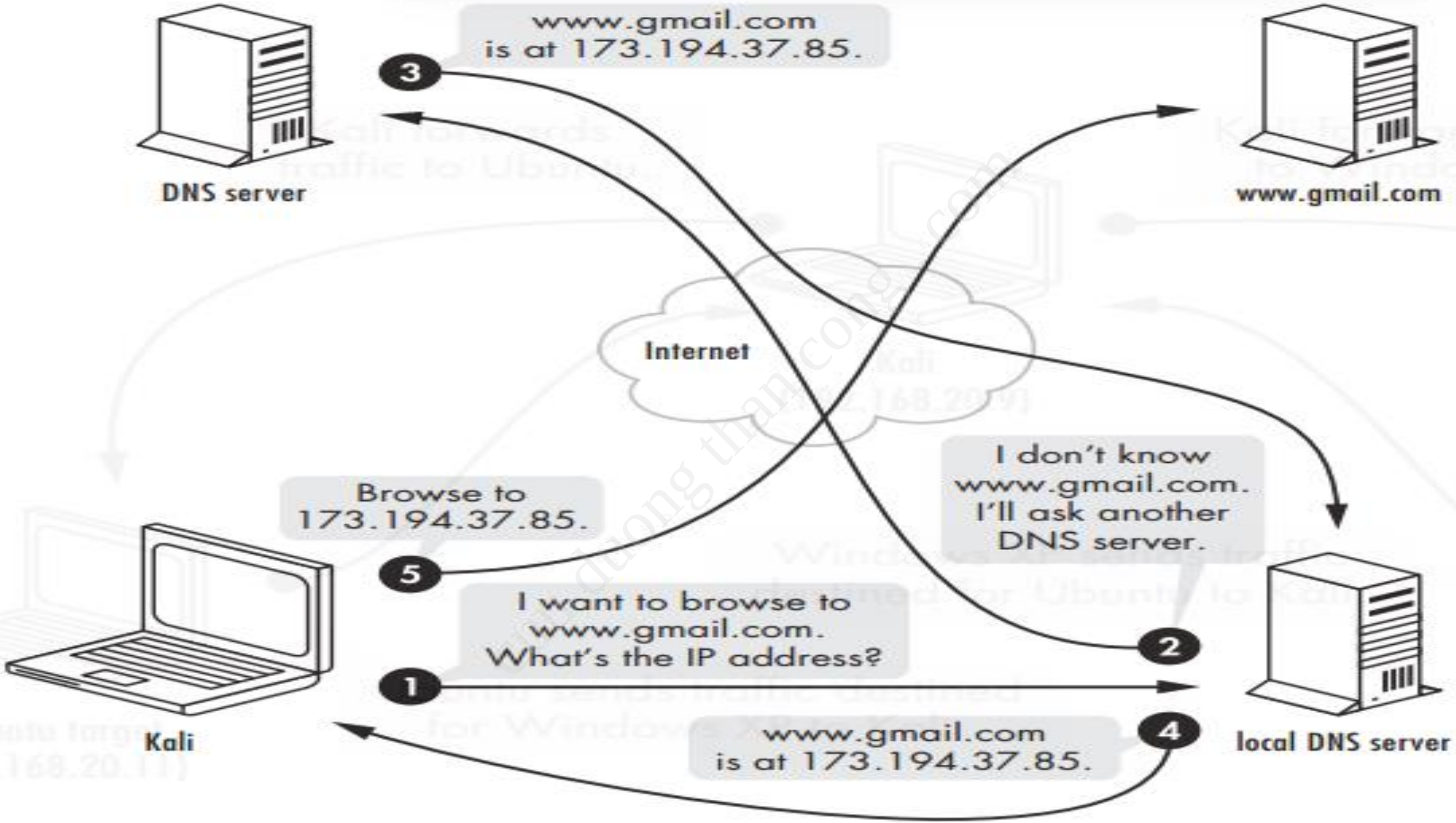
- To capture traffic not intended for the Kali system, we need to find some way to have the relevant data sent to our Kali system.
- Perform a man-in-the-middle attack: redirect and intercept traffic between two systems





DNS Cache Poisoning

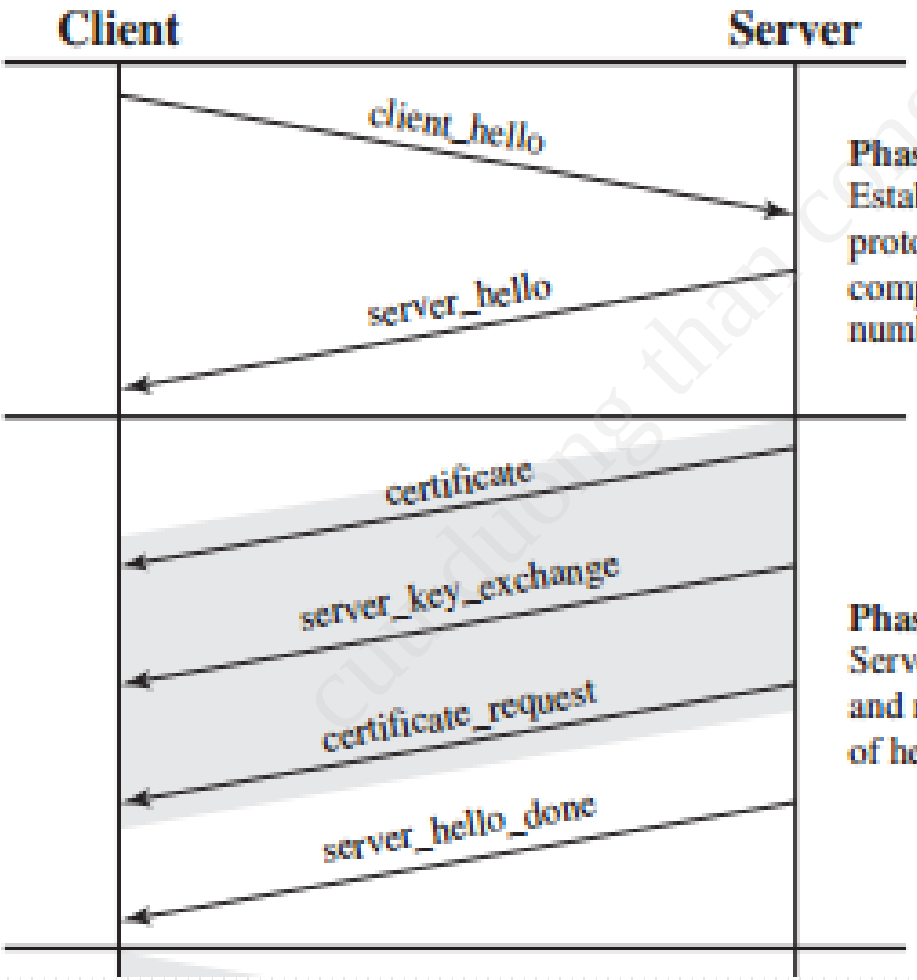
- We can poison Domain Name Service (DNS) cache entries (mappings from domain names to IP addresses) to route traffic intended for another website to one we control.
- We send a bunch of bogus DNS resolution replies pointing to the wrong IP address for a domain name



3. SSL Man-in-the-Middle Attacks

- The goal of SSL is to provide reasonable assurance that any sensitive information transmitted between a user's browser and a server is secure - unable to be read by a malicious entity along the way.

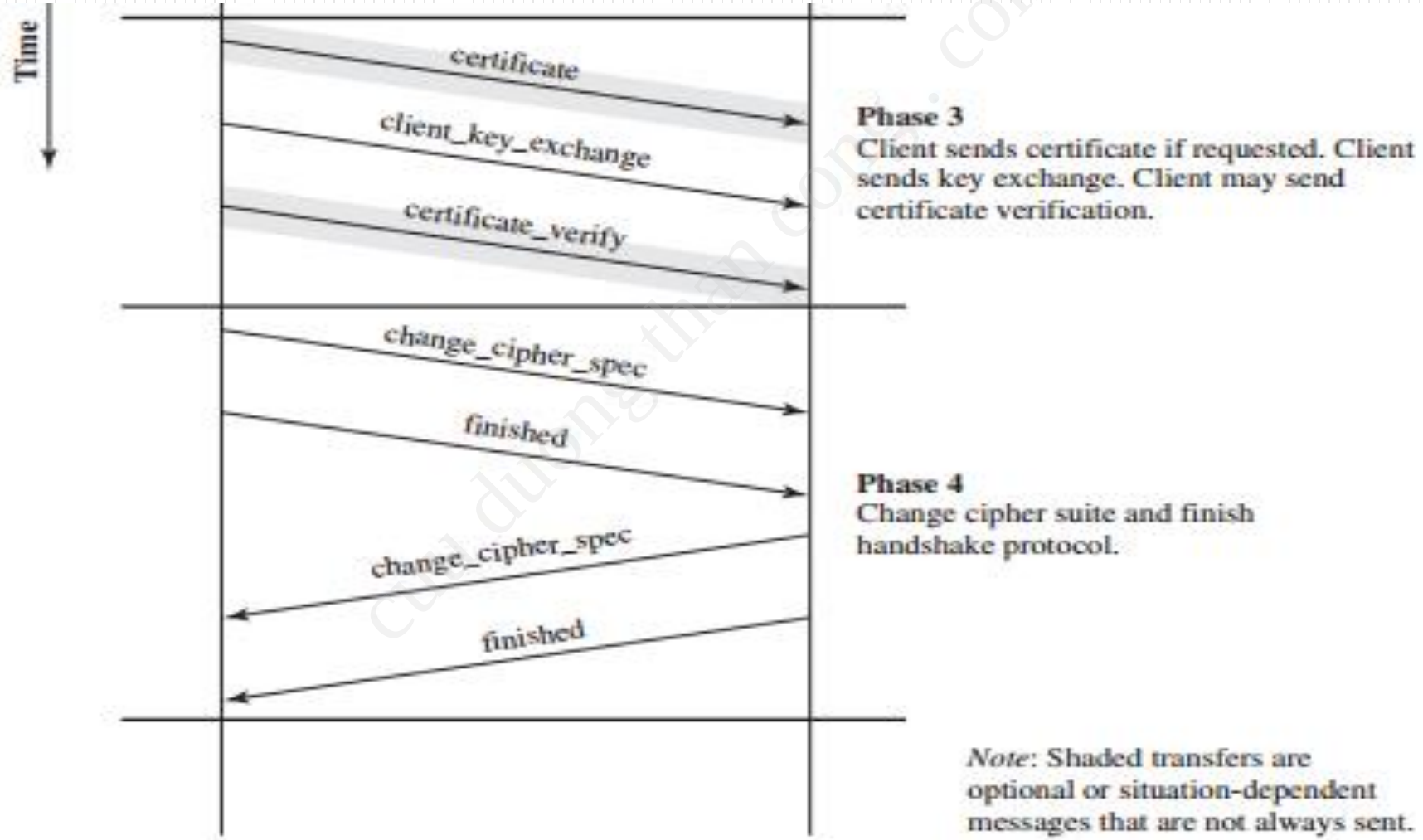
How SSL work



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

How SSL work



SSL Man-in-the-Middle Attacks