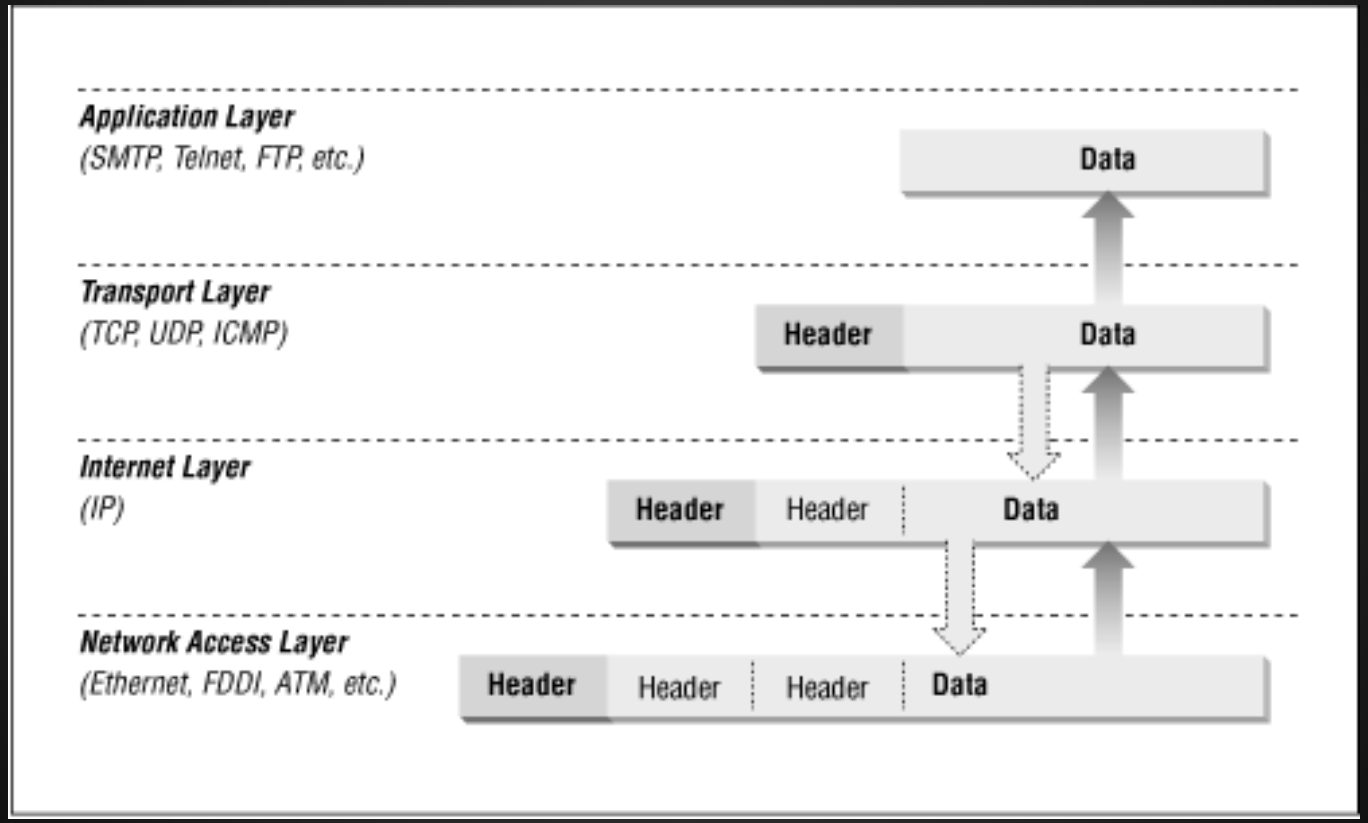
Introduction to Wireless Network Hacking

(relevant to Lab 3)

Networking Refresher

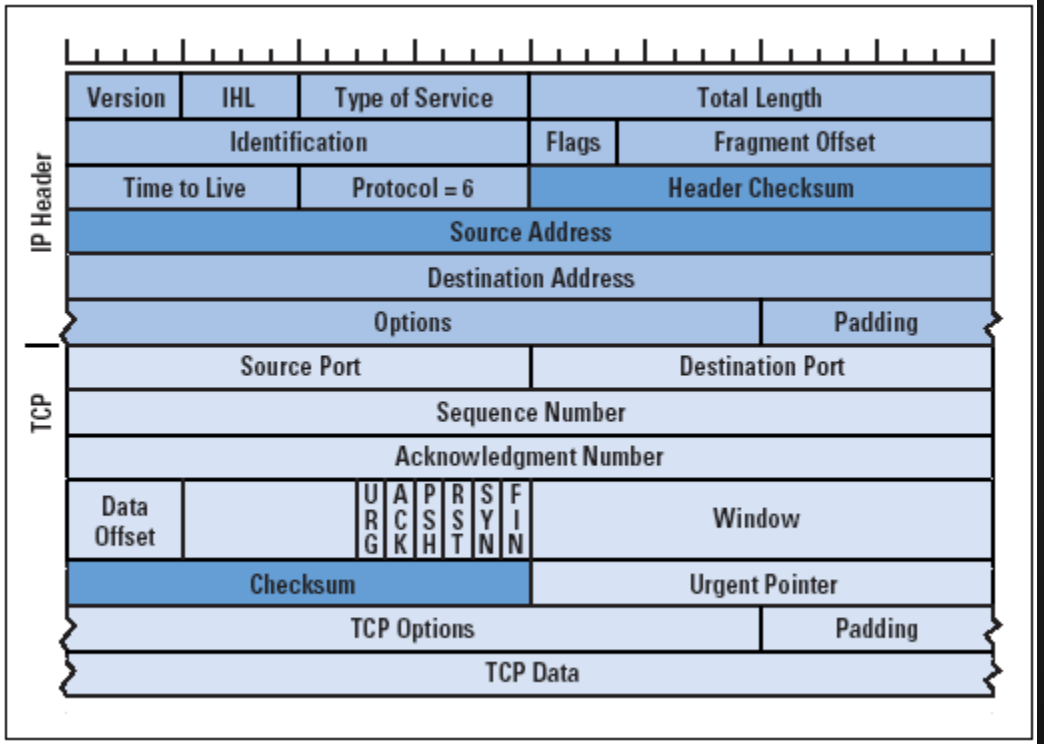
Encapsulation



http://books.gigatux.nl/mirror/snortids/0596006616/snortids-CHP-2-SECT-2.html

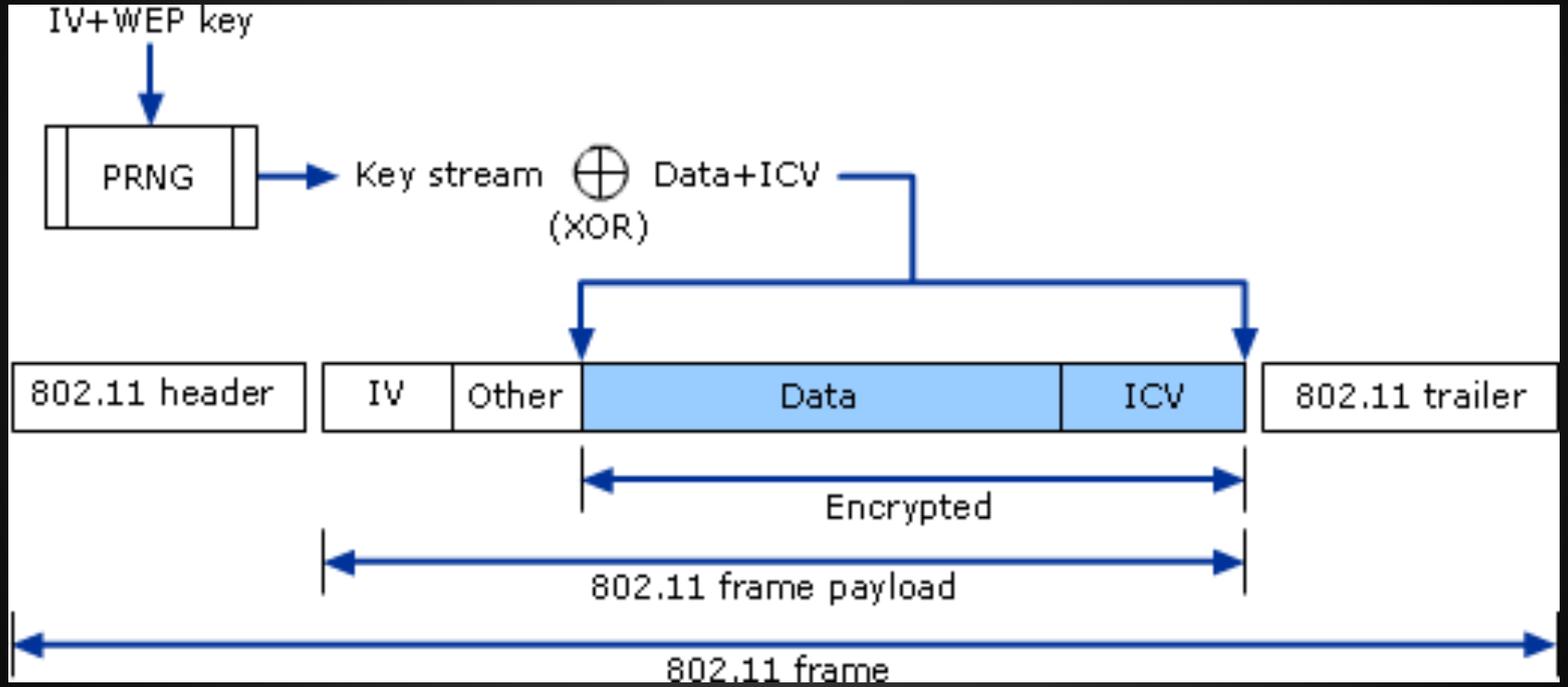
TCP/IP Packet

Figure 1: TCP/IP Header Fields Altered by NATs (Outgoing Packet)



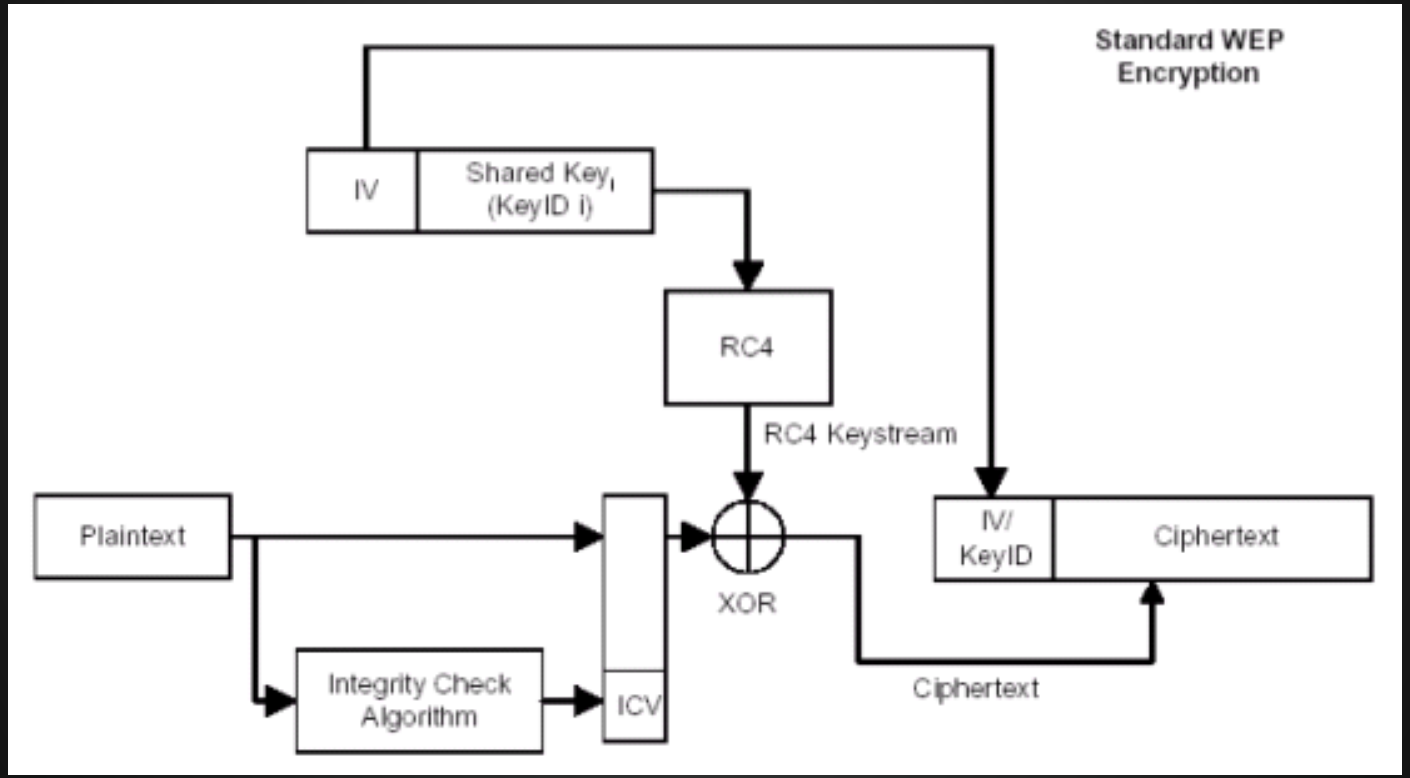
http://erlerobotics.gitbooks.io/erle-robotics-introduction-to-linux-networking/content/introduction_to_network/img/packet.gif

WEP Frame



https://i-technet.sec.s-msft.com/dynimg/IC196394.gif

WEP Encryption (frame payload)



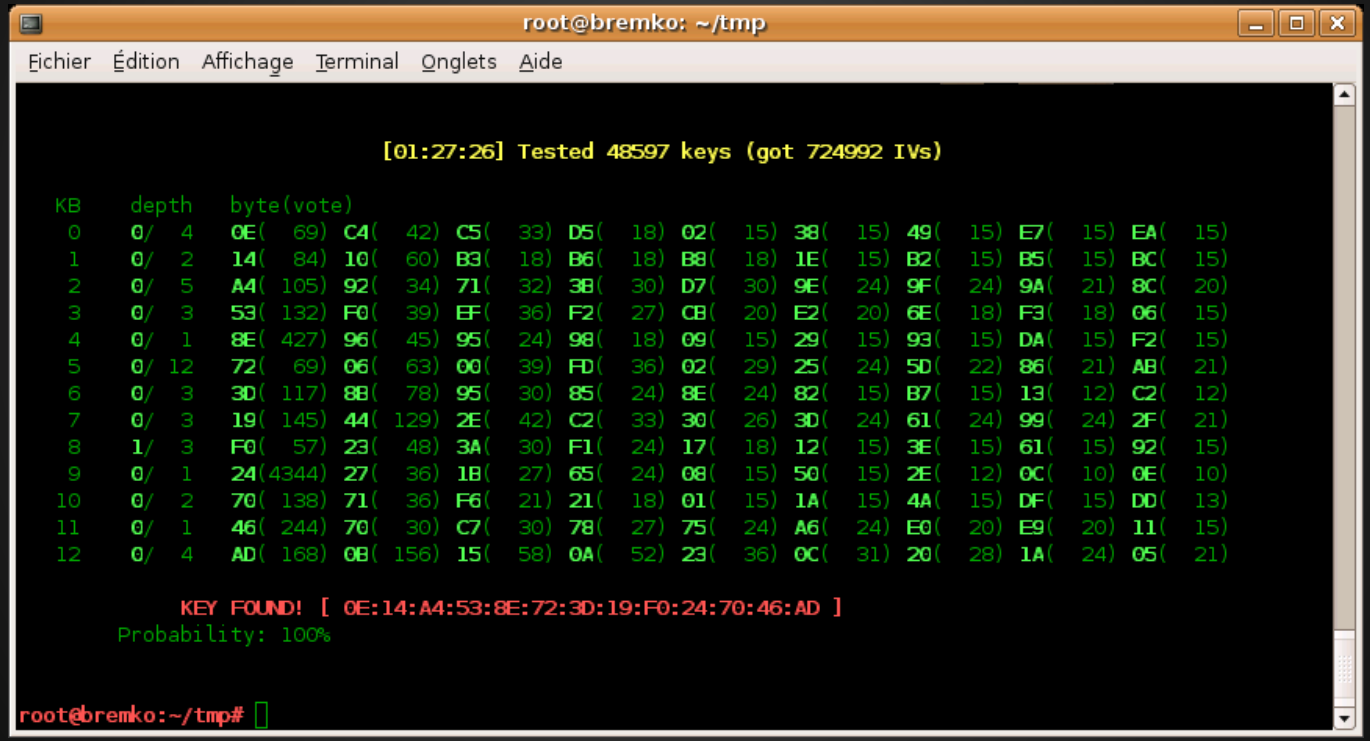
http://www.wirelessdevnet.com/articles/80211security/img2.gif

Kismet

802.11 layer2 wireless network detector, sniffer, and intrusion detection system

Aircrack-ng

Docs: http://www.aircrack-ng.org/doku.php?id=simple_wep_crack



http://www.davidgis.fr/download/img/aircrack-ng-wep3.png

Aircrack Workflow

1. Put card in monitor mode on desired channel
   a. use airmon-ng
2. Capture IVs
   a. use airodump-ng
3. If you need more IVs, then inject (you won't for lab 3)
   a. use aireplay-ng
4. When you have enough IVs, then crack
   a. use aircrack-ng

Kali

https://www.kali.org

Wireshark

network protocol analyzer

Nmap

“security scanner for network exploration and hacking”

nmap

Usage: nmap [Scan Type(s)] [Options] {target(s)}

eg: `$ sudo nmap -Pn -A 192.168.99.100`

Useful scan types:

- -Pn: skip ping probes
- -sS: SYN scan
- -A: Aggressive - OS fingerprinting, service versions, traceroutes, runs script scans


PORT SCANNING
IS NOT A CRIME


M3
PORT SCANNING
IS NOT A CRIME

Actually, maybe it is...

check your international, federal, state and local laws and university guidelines, etc

Scapy

network packet manipulation in python

Scapy

Check the docs for usage: http://www.secdev.org/projects/scapy/doc/

Example commands:

Read in a pcap:	`>>> cap = rdpcap('/tmp/p.pcap')`
Reference 11th packet:	`>>> p = cap[10]`
Show packet info:	`>>> p.show()`
Set a packet property:	`>>> p.dst = 'fe:ed:fa:ce:ee:ee'`
Send a packet:	`>>> send(p)`
Make send/recv diagram:	`>>> cap.conversations()`

Happy Hacking!