Wireless Network Esercitazioni

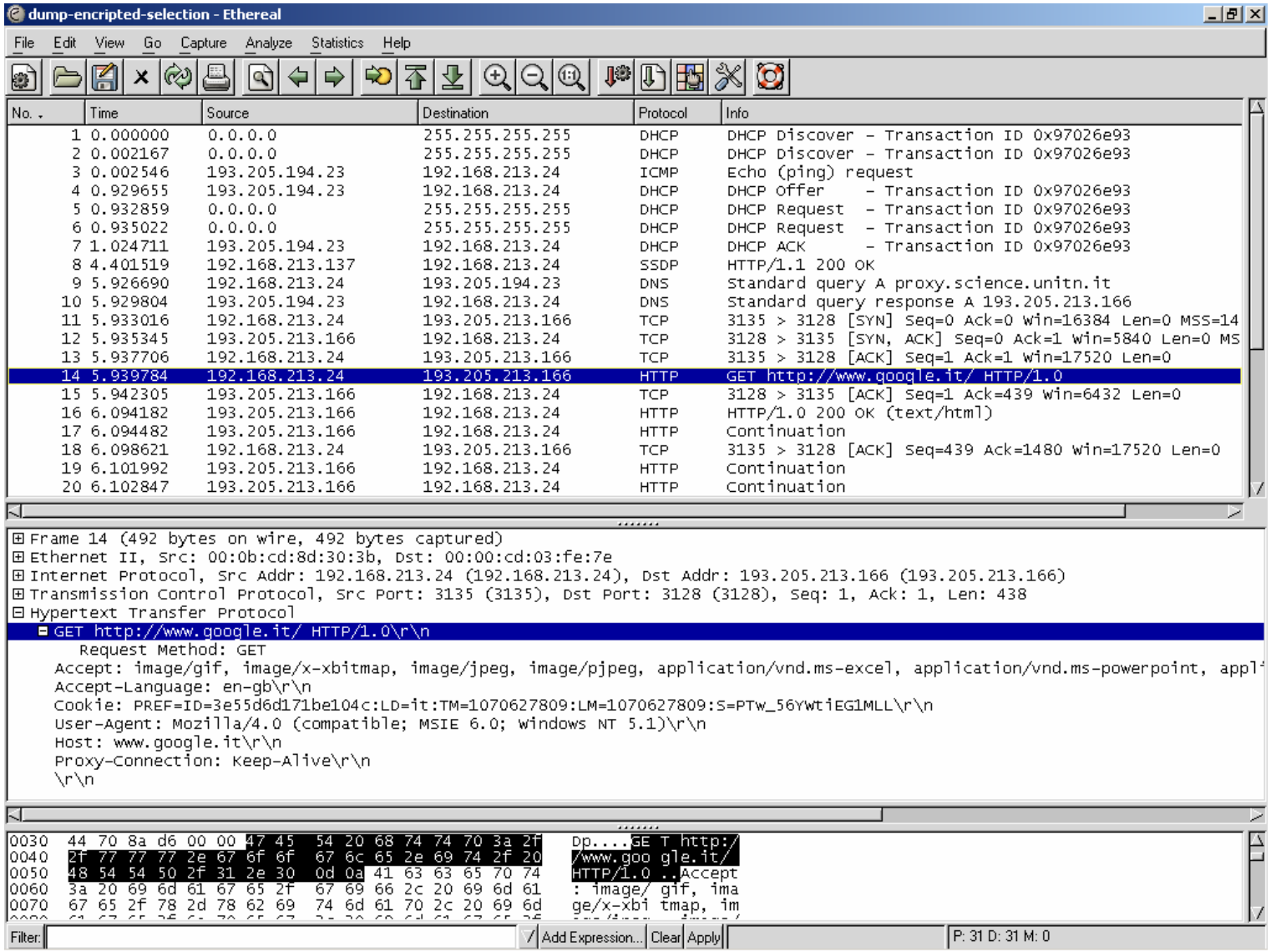
Alessandro Villani
avillani@science.unitn.it

Ethereal

Ethereal: Sniffing sullo stesso AP

- AP X con chiave WEP
- Client A connesso wireless all'AP X
- Client B connesso wireless all'AP X
- B con ethereal
- B riesce a catturare tutto il traffico di A!

Ethereal: Sniffing sullo stesso AP



Ethereal: Sniffing sullo stesso AP

- Seguendo le sessioni si ottiene:

```
GET http://www.google.it/ HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
    excel, application/vnd.ms-powerpoint, application/msword, application/x-
    shockwave-flash, */*
Accept-Language: en-gb
Cookie:
    PREF=ID=3e55d6d171be104c:LD=it:TM=1070627809:LM=1070627809:S=PTw_56YWtiEG1MLL
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: www.google.it
Proxy-Connection: Keep-Alive

HTTP/1.0 200 OK
Cache-Control: private
Content-Type: text/html
Server: GWS/2.1
Content-Length: 3039
Date: Wed, 12 May 2004 15:03:46 GMT
X-Cache: MISS from proxy.science.unitn.it
Proxy-Connection: keep-alive

<html><head><meta http-equiv="content-type" content="text/html; charset=UTF-
    8"><title>Google</title><style><!--body,td,a,p,.h{font-family:arial,sans-
    serif;}.h{font-size: 20px;}.q{color:#0000cc;}//--></style><script><!--function
```

Ethereal: Accounting su AP Cisco

Richiesta di Accounting (Code = 4): Start

```
Frame 1 (242 bytes on wire, 242 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.32 (172.31.194.32), Dst Addr: 192.168.194.168
    (192.168.194.168)
User Datagram Protocol, Src Port: 2375 (2375), Dst Port: radacct (1813)
Radius Protocol
    Code: Accounting Request (4)
    Packet identifier: 0x1 (1)
    Length: 200
    Authenticator: 0xE8B22BAA94A8C9C33513B03547064CA7
    Attribute value pairs
        t:Acct Status Type(40) l:6, Value:Start(1)
        t:User Name(1) l:14, Value:"000bcd8d303b"
        t:Acct Session Id(44) l:10, Value:"  700001"
        t:Acct Authentic(45) l:6, Value:Local(2)
        t:NAS Port(5) l:6, Value:37
        t:Calling Station Id(31) l:14, Value:"000bcd8d303b"
        t:NAS identifier(32) l:15, Value:"CISCO 350 - 2"
        t:NAS IP Address(4) l:6, Value:172.31.194.32
        t:Vendor Specific(26) l:17, Vendor:Cisco(9)
            t:Cisco AV Pair(1) l:11, Value:"vlan-id=0"
        t:Vendor Specific(26) l:34, Vendor:Cisco(9)
            t:Cisco AV Pair(1) l:28, Value:"nas-location=Malga - Atrio"
        t:Vendor Specific(26) l:27, Vendor:Cisco(9)
            t:Cisco AV Pair(1) l:21, Value:"auth-algo-type=open"
        t:Vendor Specific(26) l:19, Vendor:Cisco(9)
            t:Cisco AV Pair(1) l:13, Value:"ssid=WNTEST"
        t:Acct Delay Time(41) l:6, Value:0
```

Ethereal: Accounting su AP Cisco

Richiesta di Accounting (Code = 4): Stop

```
Frame 3 (193 bytes on wire, 193 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.32 (172.31.194.32), Dst Addr: 192.168.194.168
    (192.168.194.168)
User Datagram Protocol, Src Port: 2378 (2378), Dst Port: radacct (1813)
Radius Protocol
    Code: Accounting Request (4)
    Packet identifier: 0x2 (2)
    Length: 151
    Authenticator: 0x0D7AA97243A5E220748D78B57A306BFE
    Attribute value pairs
        t:Acct Status Type(40) l:6, Value:Stop(2)
        t:User Name(1) l:14, Value:"000bcd8d303b"
        t:Acct Session Id(44) l:10, Value:"  700001"
        t:Acct Authentic(45) l:6, Value:Local(2)
        t:Acct Input Octets(42) l:6, Value:2406852
        t:Acct Output Octets(43) l:6, Value:100908
        t:Acct Input Packets(47) l:6, Value:2495
        t:Acct Input Gigawords(52) l:6, Value:0
        t:Acct Output Gigawords(53) l:6, Value:0
        t:Acct Output Packets(48) l:6, Value:521
        t:Acct Session Time(46) l:6, Value:125
        t:NAS Port(5) l:6, Value:37
        t:Calling Station Id(31) l:14, Value:"000bcd8d303b"
        t:NAS identifier(32) l:15, Value:"CISCO 350 - 2"
        t:NAS IP Address(4) l:6, Value:172.31.194.32
        t:Acct Terminate Cause(49) l:6, Value:Lost Carrier(2)
        t:Acct Delay Time(41) l:6, Value:2
```

IAPP – 802.11F

802.11F

- L'idea è quella di definire una raccomandazione "pratica" per l'implementazione di un Inter-Access Point Protocol (IAPP) su un Distribution System (DS) su wireless LAN (WLAN)
- Non è ancora realmente utilizzato
- Scaricabile all'indirizzo: http://standards.ieee.org/getieee802/download/802.11F-2003.pdf

802.11F

- Una ESS è un insieme di BSS che formano una singola LAN, permettendo ad una stazione di muoversi trasparentemente da una BSS ad un'altra attraverso l'ESS
- L'inizializzazione del primo AP stabilisce la formazione di una ESS. I successivi AP interconnessi da un DS comune e che utilizzano lo stesso SSID, estendono la ESS creata da primo

802.11F

- IAPP è definito in modo da fornire un meccanismo sicuro per l'handoff delle informazioni sulle stazioni tra AP della stessa ESS
- IAPP può usare un server RADIUS per definire gli AP membri di una ESS.

802.11F

- Definisce tutta una serie di primitive per gestire l'ESS. Ad esempio:
  - **IAPP-MOVE.indication:** questa primitiva è utilizzata per indicare che una stazione si è riassociata con un altro AP.
  - **IAPP-MOVE.response:** questa primitiva è utilizzata per inviare ogni informazione rilevante residente nell'AP ad un'altro AP quando una stazione si è riassociata con questo secondo AP.

802.11F: AP Avaya

- Ad esempio gli AP3 Avaya trasmettono in multicast le informazioni seguenti:

```
Frame 1107 (104 bytes on wire, 104 bytes captured)
Ethernet II, Src: 00:02:2d:71:09:8e, Dst: 01:00:5e:00:01:4c
Internet Protocol, Src Addr: 172.31.194.14 (172.31.194.14), Dst Addr:
   224.0.1.76 (224.0.1.76)
User Datagram Protocol, Src Port: 2313 (2313), Dst Port: 2313 (2313)
Inter-Access-Point Protocol
    Version: 1
    Type: Announce Response(1)
    Protocol data units
        BSSID(1) Value: 00:02:2d:8a:44:ba
        Capabilities(4) Value: bf (WEP)
        PHY Type(16) Value: DSSS
        Announce Interval(5) Value: 120 seconds
        Handover Timeout(6) Value: 512 Kus
        ELSA Authentication Info(129) Value:
        Regulatory Domain(17) Value: ETSI (Europe)
        Radio Channel(18) Value: 7
        Beacon Interval(19) Value: 100 Kus
        Network Name(0) Value: "WILMA\000"
```

802.11F: AP DLink

- Ad esempio gli AP1000+ DLink trasmettono in broadcast le informazioni seguenti:

```
Frame 86 (89 bytes on wire, 89 bytes captured)
Ethernet II, Src: 00:80:c8:b8:40:77, Dst: ff:ff:ff:ff:ff:ff
Internet Protocol, Src Addr: 172.31.194.41 (172.31.194.41), Dst Addr:
   255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 2313 (2313), Dst Port: 2313 (2313)
Inter-Access-Point Protocol
    Version: 0
    Type: Announce Request(0)
    Protocol data units
        Network Name(0) Value: "FAUSTO"
        BSSID(1) Value: 00:80:c8:b8:40:77
        Capabilities(4) Value: 40 (Forwarding)
        Announce Interval(5) Value: 12294 seconds
        Handover Timeout(6) Value: 1799 Kus
        Message ID(7) Value: 100
        Unknown PDU Type(124) Value:
        Unknown PDU Type(125) Value:
```

Kismet

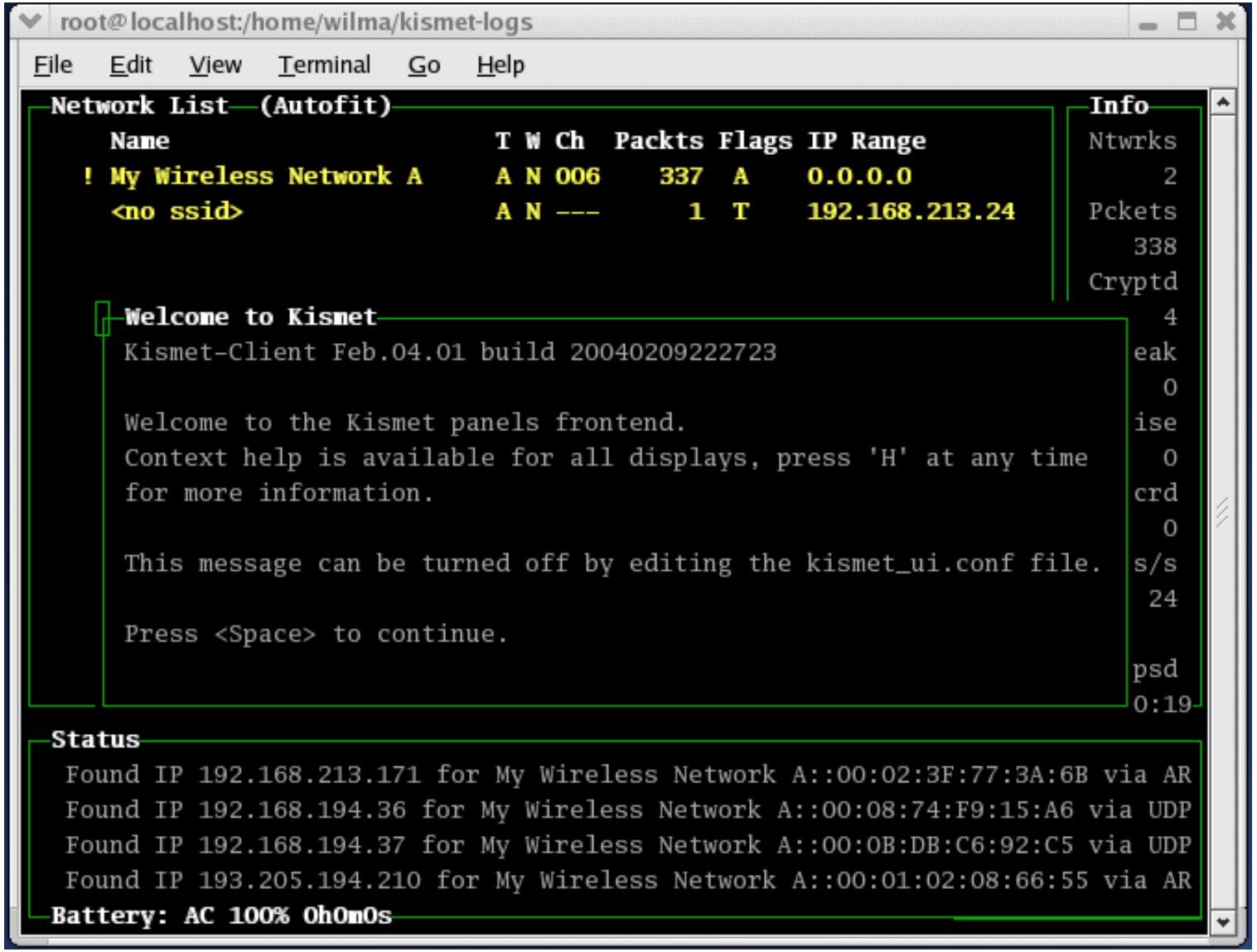
Kismet

- Kismet è un packet sniffer per 802.11 che gira sotto linux
- Consente di analizzare il layer 2
- Può essere scaricato all'indirizzo:
  http://www.kismetwireless.net/
- Per funzionare richiede di utilizzare delle schede wireless che supportano la modalità di raw monitoring

Kismet

- In generale si devono installare driver particolari, quali wlan-ng:
  ftp://ftp.linux-wlan.org/pub/linux-wlan-ng/
- La procedura di installazione non è molto semplice e richiede una certa cautela ed esperienza.
- Anche l'interfaccia è molto spartana
- Kismet produce dei dump files che poi possono essere interpretati da ethereal

Kismet


root@localhost:/home/wilma/kismet-logs
File Edit View Terminal Go Help
Network List (Autofit)
Name T W Ch Packts Flags IP Range
! My Wireless Network A A N 006 337 A 0.0.0.0
<no ssid> A N --- 1 T 192.168.213.24
Info
Ntwrks
2
Pckets
338
Cryptd
4
Welcome to Kismet
Kismet-Client Feb.04.01 build 20040209222723
Welcome to the Kismet panels frontend.
Context help is available for all displays, press 'H' at any time
for more information.
This message can be turned off by editing the kismet_ui.conf file.
Press <Space> to continue.
Status
Found IP 192.168.213.171 for My Wireless Network A::00:02:3F:77:3A:6B via AR
Found IP 192.168.194.36 for My Wireless Network A::00:08:74:F9:15:A6 via UDP
Found IP 192.168.194.37 for My Wireless Network A::00:0B:DB:C6:92:C5 via UDP
Found IP 193.205.194.210 for My Wireless Network A::00:01:02:08:66:55 via AR
Battery: AC 100% OhOmOs

Kismet: Frame 802.11

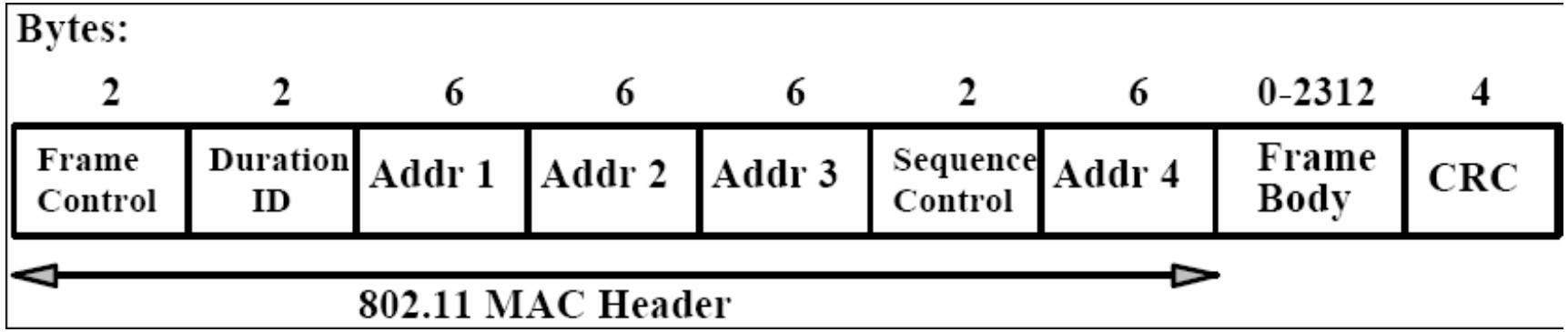
- Kismet ci consente di analizzare i frame di una comunicazione 802.11
- 802.11 definisce vari tipi di frame che le stazioni (NIC e AP) usano per comunicare fra loro, così come per gestire e controllare il link wireless.

Kismet: Frame 802.11

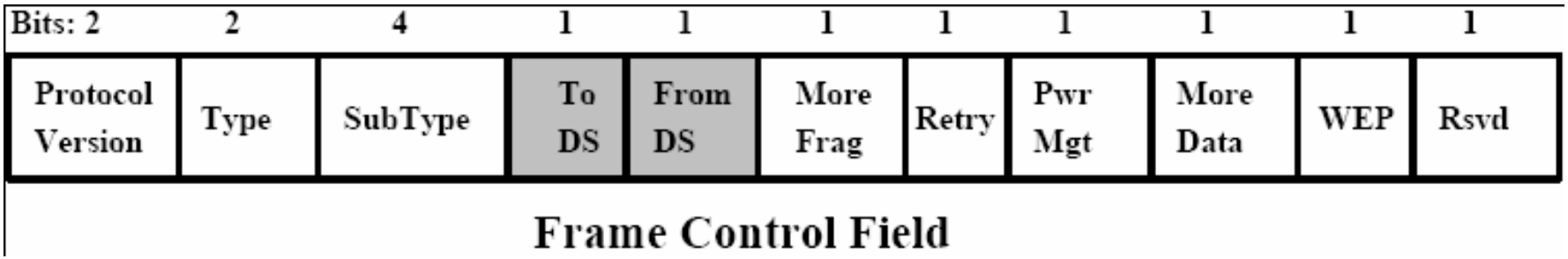
- Ciascun frame ha un campo di controllo che definisce la versione del protocollo 802.11, il tipo di frame, e vari indicatori, quali se il WEP è attivo, se il power management è attivo, ...
- Ogni frame contiene i MAC addresses delle stazioni sorgenti e destinazioni, un numero di frame, il corpo del frame e un frame check (per il controllo degli errori).

Kismet: Frame 802.11

- Frame format:



- Il Frame Control Field è:



Kismet: Frame 802.11

- Frame Management

Type Value	Type Description	Subtype Value	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Ressociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1110-1111	Reserved

Kismet: Frame 802.11

- Frame Control

Type Value	Type Description	Subtype Value	Subtype Description
01	Control	0000-1001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1101	CF End
01	Control	1111	CF End + CF-ACK

Kismet: Frame 802.11

- Frame Data

Type Value	Type Description	Subtype Value	Subtype Description
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-ACK + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved

Kismet: Frame 802.11

- **Management Frames:** consentono di stabilire e mantenere le comunicazioni. Ad esempio:
  - **Authentication frame**: la NIC comincia il processo di autenticazione mandando all'AP un frame di autenticazione contenente la propria identità
    - Open system: la NIC manda unicamente un authentication frame, e l'AP risponde con un authentication frame indicando l'accettazione o meno.
    - Shared key: la NIC manda inizialmente un frame di authentication frame, e l' AP risponde con un authentication frame contenente una challenge. La NIC deve mandare indietro una versione crittata della challenge (utilizzando la chiave WEP) in un authentication frame.

Kismet: Frame 802.11

- **Deauthentication frame**
- **Association request frame:** Permette all'AP di allocare risorse per una NIC.
  Una NIC comincia il processo di associazione mandando una association request ad un AP. Questo frame porta informazioni sulla NIC (ad esempio le data rates supportate) e la SSID della rete a cui si vuole associare.
- **Association response frame**: Un AP invia un *association response frame* contenente una notifica di accettazione o respinta alla richiesta di associazione della NIC. Se l'AP accetta la NIC, il frame include informazioni quali l'association ID e le data rates supportate.

Kismet: Frame 802.11

- **Beacon frame**: L'AP manda periodicamente un *beacon frame* per annunciare la sua presenza e inviare informazioni, quali timestamp, SSID, e altri parametri riguardanti l'AP
- **Probe request frame**: Una stazione manda un *probe request frame* quando ha bisogno di ottenere informazioni da un'altra stazione.
- **Probe response frame**: Una stazione risponderà con un *probe response frame*, contenente informazioni quali le velocità supportate, in seguito alla ricezione di un *probe request frame*.

Kismet: Frame 802.11

- **Control Frames:** utilizzati nella consegna dei data frames fra le stazioni. Ad esempio:
  - **Request to Send (RTS) frame**
  - **Clear to Send (CTS) frame**
  - **Acknowledgement (ACK) frame**: dopo la ricezione di un *data frame*, la stazione ricevente utilizzerà un processo di error checking ed invierà un *ACK frame* alla stazione trasmittente se non ci sono errori. Se la stazione trasmittente non riceve un ACK dopo un certo tempo ritrasmetterà il frame.

Kismet: Frame 802.11

- **Data Frames**: il data frame trasporta i pacchetti dai livelli più alti, come pagine web, informazioni di controllo per le stampanti, ..., all'onterno del corpo del frame.

Kismet: Frame 802.11

- **ToDS:**
  - questo bit è a 1 quando il frame è diretto all'AP per il forwarding al DS
  - Il bit è a 0 in tutti gli altri casi
- **FromDS:**
  - questo bit è a 1 quando il frame è ricevuto dal DS
  - Il bit è a 0 in tutti gli altri casi

Kismet: Frame 802.11

- **More Fragments:**
  - questo bit è a 1 quando ci sono più frammenti appartenenti allo stesso frame che seguono il frame attuale
- **Retry:**
  - questo bit indica che questo frame è la ritrasmissione di un frame precedentemente trasmesso. Utilizzato dalla stazione ricevente per rendersi conto di ritrasmissioni dovute alla perdita di ACK
- **Power Management:**
  - questo bit indica quale sarà il *Power Management mode* della stazione dopo la trasmissione di questo frame

Kismet: Frame 802.11

- **More Data:**
  - questo bit è utilizzato sia per il *Power Management* come dall'AP che ci sono ancora frame per questa stazione nel buffer. La stazione può decidere di usare l'informazione per continuare il polling o passare in Active mode.
- **WEP:**
  - Questo bit indica che il frame body è crittato con WEP
- **Order:**
  - Questo bit indica che il frame è inviato utilizzando *Strictly-Ordered service class*

Kismet: Frame 802.11

- **Duration/ID:**
  - Questo campo a due significati a seconda del tipo di frame:
    - In un messaggio Power-Save Poll corrisponde alla Station ID
    - In tutti gli altri frames questa è la durata utilizzata per il calcolo della NAV
- **Sequence Control:**
  - Questo campo è usato per rappresentare l'ordine di diversi frammenti appartenenti allo stesso frame e per riconoscere pacchetti duplicati.
    Consiste di due sottocampi: *Fragment Number* e *Sequence Number*.

Kismet: Frame 802.11

- **Address Fields:**
  - Un frame può contenere fino a 4 indirizzi in base al valore di ToDS e FromDS bits:
    - **Address-1** è sempre l'indirizzo del destinatario.
      Se ToDS è a 1 allora è l'indirizzo dell'AP, altrimenti è l'indirizzo della stazione finale
    - **Address-2** è sempre l'indirizzo del trasmittente.
      Se FromDS è a 1 allora è l'indirizzo dell'AP, altrimenti è l'indirizzo della stazione finale
    - **Address-3** di solito è l'indirizzo della AP.
      Se FromDS è 1 Address-3 è l'indirizzo sorgente originale,
      Se ToDS è 1 allora Address 3 è l'indirizzo desatinazione.
    - **Address-4** è usato in casi speciali quando è usato un Wireless Distribution Systemed il frame è trasmesso da un AP ad un'altro

Kismet: Frame 802.11

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Kismet: Beacon Frame – Parte 1

```
Frame 1 (74 bytes on wire, 74 bytes captured)
    Arrival Time: May 12, 2004 19:47:45.608790000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 74 bytes
    Capture Length: 74 bytes
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 8
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
   From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    Source address: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Fragment number: 0
    Sequence number: 3331
```

Kismet: Beacon Frame – Parte 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000000002A29C181
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0021
            .... .... .... ...1 = ESS capabilities: Transmitter is an AP
            .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
            .... .... .... 00.. = CFP participation capabilities: No point coordinator
    at AP (0x0000)
            .... .... ...0 .... = Privacy: AP/STA cannot support WEP
            .... .... ..1. .... = Short Preamble: Short preamble allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... .0.. .... .... = Short Slot Time: Short slot time not in use
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
    Tagged parameters (38 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 21
        Tag interpretation: My Wireless Network A
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 6
        Tag Number: 5 ((TIM) Traffic Indication Map)
        Tag length: 4
        Tag interpretation: DTIM count 0, DTIM period 1, Bitmap control 0x0, (Bitmap
    suppressed)
```

Kismet: Probe Request – Parte 1

```
Frame 544 (32 bytes on wire, 32 bytes captured)
    Arrival Time: May 12, 2004 19:48:13.459572000
    Time delta from previous packet: 0.007184000 seconds
    Time since reference or first frame: 27.850782000 seconds
    Frame Number: 544
    Packet Length: 32 bytes
    Capture Length: 32 bytes
IEEE 802.11
    Type/Subtype: Probe Request (4)
    Frame Control: 0x0040 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 4
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
   From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    Source address: 00:0b:cd:8d:30:3b (CompaqHp_8d:30:3b)
    BSS Id: ff:ff:ff:ff:ff:ff (Broadcast)
    Fragment number: 0
    Sequence number: 2065
```

Kismet: Probe Request – Parte 2

```
IEEE 802.11 wireless LAN management frame
    Tagged parameters (8 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 0
        Tag interpretation:
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]
```

Kismet: Probe Response – Parte 1

```
Frame 546 (68 bytes on wire, 68 bytes captured)
    Arrival Time: May 12, 2004 19:48:13.461723000
    Time delta from previous packet: 0.001182000 seconds
    Time since reference or first frame: 27.852933000 seconds
    Frame Number: 546
    Packet Length: 68 bytes
    Capture Length: 68 bytes
IEEE 802.11
    Type/Subtype: Probe Response (5)
    Frame Control: 0x0050 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 5
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
   From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 314
    Destination address: 00:0b:cd:8d:30:3b (CompaqHp_8d:30:3b)
    Source address: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Fragment number: 0
    Sequence number: 3863
```

Kismet: Probe Response – Parte 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000000002BD2C1BD
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0021
            .... .... .... ...1 = ESS capabilities: Transmitter is an AP
            .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
            .... .... .... 00.. = CFP participation capabilities: No point coordinator
    at AP (0x0000)
            .... .... ...0 .... = Privacy: AP/STA cannot support WEP
            .... .... ..1. .... = Short Preamble: Short preamble allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... .0.. .... .... = Short Slot Time: Short slot time not in use
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
    Tagged parameters (32 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 21
        Tag interpretation: My Wireless Network A
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 6
```

Kismet: Auth. Request – Parte 1

```
Frame 1075 (30 bytes on wire, 30 bytes captured)
    Arrival Time: May 12, 2004 16:51:30.631147000
    Time delta from previous packet: 0.067849000 seconds
    Time since reference or first frame: 56.851711000 seconds
    Frame Number: 1075
    Packet Length: 30 bytes
    Capture Length: 30 bytes
IEEE 802.11
    Type/Subtype: Authentication (11)
    Frame Control: 0x00B0 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 11
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
   From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 258
    Destination address: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Source address: 00:0b:cd:8d:30:3b (172.31.194.10)
    BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Fragment number: 0
    Sequence number: 28
```

Kismet: Auth. Request – Parte 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
        Authentication Algorithm: Open System (0)
        Authentication SEQ: 0x0001
        Status code: Successful (0x0000)
```

Kismet: Ass. Request – Parte 1

```
Frame 153 (57 bytes on wire, 57 bytes captured)
    Arrival Time: May 12, 2004 16:50:41.993265000
    Time delta from previous packet: 0.128513000 seconds
    Time since reference or first frame: 8.213829000 seconds
    Frame Number: 153
    Packet Length: 57 bytes
    Capture Length: 57 bytes
IEEE 802.11
    Type/Subtype: Association Request (0)
    Frame Control: 0x0000 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 0
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
   From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 258
    Destination address: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Source address: 00:0b:cd:8d:30:3b (172.31.194.10)
    BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Fragment number: 0
    Sequence number: 29
```

Kismet: Ass. Request – Parte 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (4 bytes)
        Capability Information: 0x0011
            .... .... .... ...1 = ESS capabilities: Transmitter is an AP
            .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
            .... .... .... 00.. = CFP participation capabilities: No point coordinator
    at AP (0x0000)
            .... .... ...1 .... = Privacy: AP/STA can support WEP
            .... .... ..0. .... = Short Preamble: Short preamble not allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... .0.. .... .... = Short Slot Time: Short slot time not in use
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
        Listen Interval: 0x0001
    Tagged parameters (29 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 21
        Tag interpretation: My Wireless Network A
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]
```

Kismet: Ass. Response – Parte 1

```
Frame 155 (36 bytes on wire, 36 bytes captured)
    Arrival Time: May 12, 2004 16:50:41.995117000
    Time delta from previous packet: 0.001237000 seconds
    Time since reference or first frame: 8.215681000 seconds
    Frame Number: 155
    Packet Length: 36 bytes
    Capture Length: 36 bytes
IEEE 802.11
    Type/Subtype: Association Response (1)
    Frame Control: 0x0010 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 1
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
   From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 314
    Destination address: 00:0b:cd:8d:30:3b (172.31.194.10)
    Source address: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Fragment number: 0
    Sequence number: 1631
```

Kismet: Ass. Response – Parte 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
        Capability Information: 0x0021
            .... .... .... ...1 = ESS capabilities: Transmitter is an AP
            .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
            .... .... .... 00.. = CFP participation capabilities: No point coordinator
    at AP (0x0000)
            .... .... ...0 .... = Privacy: AP/STA cannot support WEP
            .... .... ..1. .... = Short Preamble: Short preamble allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... .0.. .... .... = Short Slot Time: Short slot time not in use
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
        Status code: Cannot support all requested capabilities in the Capability
    information field (0x000a)
        Association ID: 0x0000
    Tagged parameters (6 bytes)
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]
```

Kismet: Data Frame (ARP) – Parte 1

```
Frame 693 (78 bytes on wire, 78 bytes captured)
    Arrival Time: May 12, 2004 19:48:17.767774000
    Time delta from previous packet: 0.006368000 seconds
    Time since reference or first frame: 32.158984000 seconds
    Frame Number: 693
    Packet Length: 78 bytes
    Capture Length: 78 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208 (Normal)
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Source address: 00:00:cd:03:fe:7e (193.205.213.1)
    Fragment number: 0
    Sequence number: 4002
Logical-Link Control
```

Kismet: Data Frame (ARP) – Parte 2

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:00:cd:03:fe:7e (193.205.213.1)
    Sender IP address: 193.205.213.1 (193.205.213.1)
    Target MAC address: ff:ff:ff:ff:ff:ff (Broadcast)
    Target IP address: 193.205.213.177 (193.205.213.177)
```

Kismet: Data Frame (Http) – Parte 1

```
Frame 1830 (510 bytes on wire, 510 bytes captured)
    Arrival Time: May 12, 2004 19:49:14.356290000
    Time delta from previous packet: 0.001401000 seconds
    Time since reference or first frame: 88.747500000 seconds
    Frame Number: 1830
    Packet Length: 510 bytes
    Capture Length: 510 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0108 (Normal)
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x1
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 258
    BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Source address: 00:0b:cd:8d:30:3b (CompaqHp_8d:30:3b)
    Destination address: 00:00:cd:03:fe:7e (193.205.213.1)
    Fragment number: 0
    Sequence number: 2078
Logical-Link Control
```

Kismet: Data Frame (Http) – Parte 2

```
Internet Protocol, Src Addr: 192.168.213.24 (192.168.213.24), Dst Addr: 193.205.213.166
    (193.205.213.166)
Transmission Control Protocol, Src Port: 3346 (3346), Dst Port: 3128 (3128), Seq: 1,
    Ack: 1, Len: 438
Hypertext Transfer Protocol
    GET http://www.google.it/ HTTP/1.0\r\n
        Request Method: GET
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
    excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-
    flash, */*\r\n
    Accept-Language: en-gb\r\n
    Cookie:
    PREF=ID=3e55d6d171be104c:LD=it:TM=1070627809:LM=1070627809:S=PTw_56YWtiEG1MLL\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n
    Host: www.google.it\r\n
    Proxy-Connection: Keep-Alive\r\n
    \r\n
```