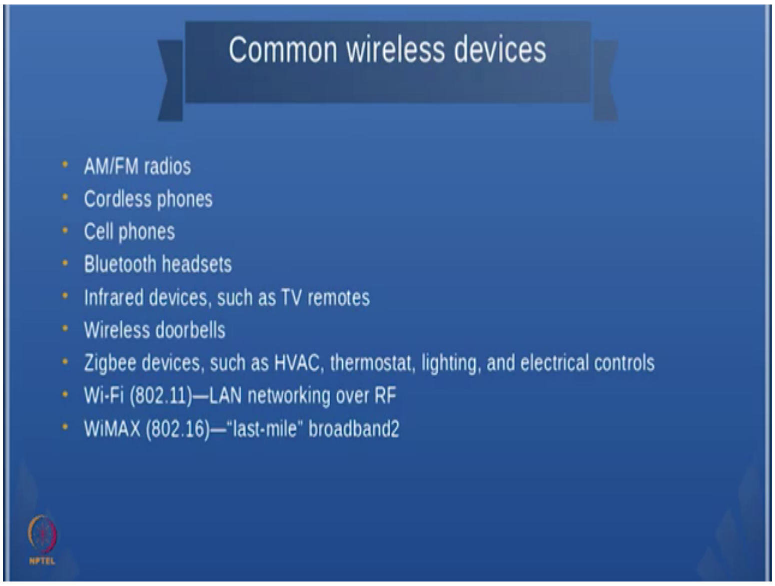
**Information security - IV**
**Prof. M J Shankar Raman**
**Department of Computer Science and Engineering**
**Indian Institute of Technology, Madras**

**Lecture – 43**
**Wireless: network forensics unplugged**
**Network Security and Forensics**

Welcome to this session on network security and forensics. Until now we saw how packets can be captured and analyzed using the different tools like wire shark, t shark etcetera ok. We saw that first is the data acquisition and once the evidence is acquired, you can actually use different kinds of tools and you can also develop your own tools to identify what is the issue and how some activity had taken place. We were mostly concentrating on wired networks.

So, we would briefly look at wireless network forensics and what are the minor differences, because there you act on wires whereas, here you act on some radio frequency networks therefore, the difference is that you need to understand about the protocols that are various protocols that are used. So, we will give you a very brief overview of various protocols, wireless protocols that are used and why we should know these protocols is that, it will be helpful for doing the right type of forensic analysis.

(Refer Slide Time: 01:37)



Common wireless devices

- AM/FM radios
- Cordless phones
- Cell phones
- Bluetooth headsets
- Infrared devices, such as TV remotes
- Wireless doorbells
- Zigbee devices, such as HVAC, thermostat, lighting, and electrical controls
- Wi-Fi (802.11)—LAN networking over RF
- WiMAX (802.16)—"last-mile" broadband2

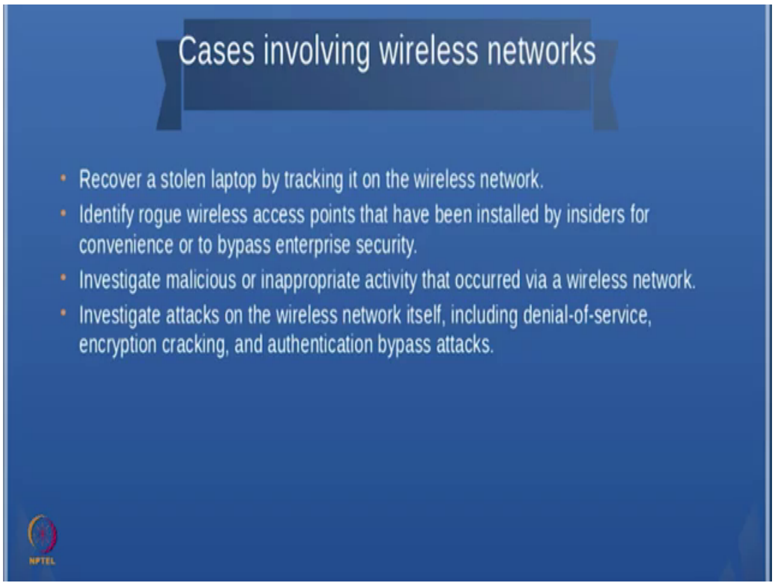
So, what we will do is, we will look at the different types of 802.11 protocols I mean different frequencies at which it operates. So, other thing that you should know is that, previously for acquiring the ethernet that we just you could have a tap and you can get the data, but here you have to connect an another device from your machine, and then try to scan what is there and then get the data whatever data is going is going through in the wireless networks ok.

So, there are many common wireless devices like am fm radios cordless phones cell phone, Bluetooth etcetera and there are also the Zigbee devices which are which are which are used for high voltage air conditioning and thermostat lighting electric controls, I mean short distance communication and then you have the Wi-Fi eight naught two dot one and then Wimax ok. And Wi-Fi is very prevalent and this is one of the security loopholes is provided by Wi-Fi. There are many cases that involve wireless networks one is you it could be a stolen laptop ok, where you could try to actually get back the laptop that is connected to a wireless network ok.

So, you could actually recover the laptop when it gets attached to a wireless networks, you could also look at some wireless rogue access points I mean it is known as something known as war driving. So, what usually these hackers do is that, they actually installed some wireless scanning do scanning software or device and then go on scanning finding out vulnerable wireless networks usually 802.11 See many of us actually give leave the default password for routers and one of the things for securities please ensure that if you are a network administrator, never leave any default installation. I think many of us feel very convenient by for by pressing the default button and then installing software and this is this can lead to lot of vulnerabilities ok. For example, a simple example is that everyone expects ssh to work on four 443 I mean so.

So, suppose I do not use the default 443, but I use some other port say some other unknown port ok. Then at least you provide a wall for the hacker to make him do some more operations rather than just barging into 4 port 443. I mean it is like providing 2 or 3 locks in your house. I mean whether it is going to ensure that a thief never enters no, but at least it can delay the entrance of the thief. So, similarly using default values for installation can lead to lot of security holes. So, please ensure that if you are a network administrator do not go for default installation, look at every installation case and see how security can be incorporated while or what are the base by which security can be enhanced by during installation by not providing default values ok.

(Refer Slide Time: 05:03)



## Cases involving wireless networks

- Recover a stolen laptop by tracking it on the wireless network.
- Identify rogue wireless access points that have been installed by insiders for convenience or to bypass enterprise security.
- Investigate malicious or inappropriate activity that occurred via a wireless network.
- Investigate attacks on the wireless network itself, including denial-of-service, encryption cracking, and authentication bypass attacks.

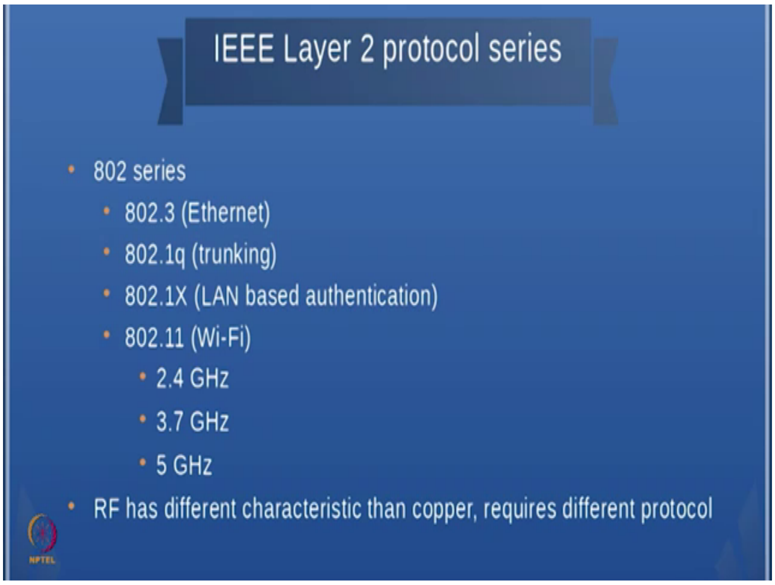
So, for example, many of the password attacks like I mean some 1 2 3 4 5 6 7 8 which is one of the most used passwords etcetera ok.

Because that could be a default and that is easy similarly admin login name admin you I mean password is admin. I think many of the wireless routers will break if you use these kinds of passwords ok. So, ensure that you do not go for this kind of default. So, what are the other things that we can do? We can actually. So, especially this kind of wireless rogue wireless access points that have been installed by insiders ok. So, many times what people will do is that, they call it as a evil twin or something ok. So, what I do is, I will install a wireless device with the same key of an official router.

So, people will think that I am the official network and they will try to connect to me thereby I can extract data from them ok. You could also there are cases that involve malicious or inappropriate activity that occurred via wireless network because I am see bring your own device kind of stuff ok. So, I bring my device which has lot of virus and then I connected the wireless network, I spread it to everyone and wireless networks are mainly open. So, unless Ethernet wire you at least you have to go to a place and then you cannot roam around here, I can actually log on to whatever place I want and then I can spread my virus happening and feel happy about it also sometimes. So, other things that you can involve other cases that were that were seen where like denial of service encryption cracking.

So, for example, I mean if I connect to my wireless network, what is the secret key I can use some scanner device and then crack some well known passwords and things that. So, I mean in wired networks its slightly difficult because you have to physically go and connect the device whereas, in wireless yes I can just have my wireless on and then do all these activities ok.

(Refer Slide Time: 07:08)



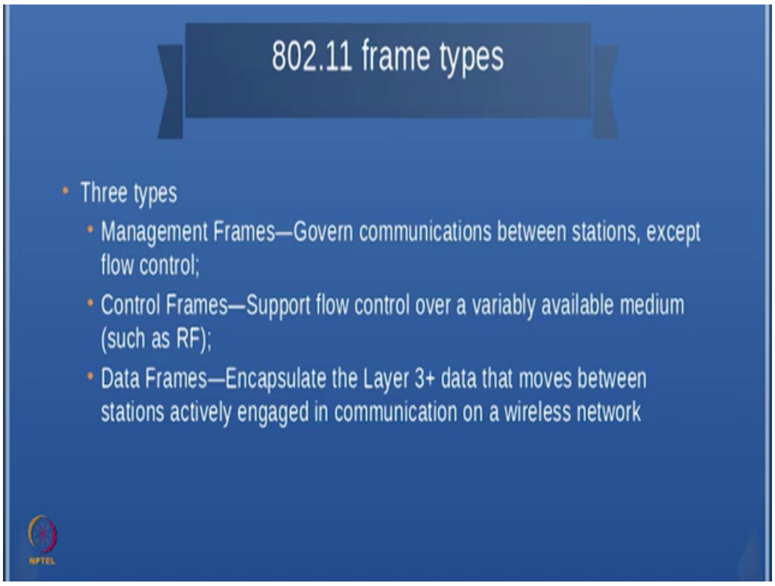
IEEE Layer 2 protocol series

- 802 series
  - 802.3 (Ethernet)
  - 802.1q (trunking)
  - 802.1X (LAN based authentication)
  - 802.11 (Wi-Fi)
    - 2.4 GHz
    - 3.7 GHz
    - 5 GHz
- RF has different characteristic than copper, requires different protocol

So,. So, wireless has a bunch of security loopholes ok. So, before we go into wireless we need to understand some of the IEEE layer two protocols ok. So, 802.3 is the Ethernet protocol. So, if you look at wire shark you would have talking about Ethernet 2 802.1 q is a trunking and then 802.1 x usually is the land based authentication and 802.11 is the Wi-Fi and it operates on 2.43. 75 usually it is 2.4 and 5 or usually used 2.4 is one which is used and if you look at this the RF has different characteristics than copper therefore, the protocols that are used are different. For example, I mean one of the places is that even TCP, we can wireless there could be much more higher amount of drops because of weak signal etcetera whereas, in Ethernet you generally do not come across those kind of problems and unless you configure it badly you mean incorrectly ok.

So, but in wireless you can have signal loss, you could have lot of retransmissions I mean. So, because of all these things what usually we do is the protocol for wireless is different from protocol that is used for Ethernet ok. So, what happens is that the wireless protocol encapsulate the Ethernet and then it transmits it in the wired networks in the in the wireless networks.

(Refer Slide Time: 08:37)

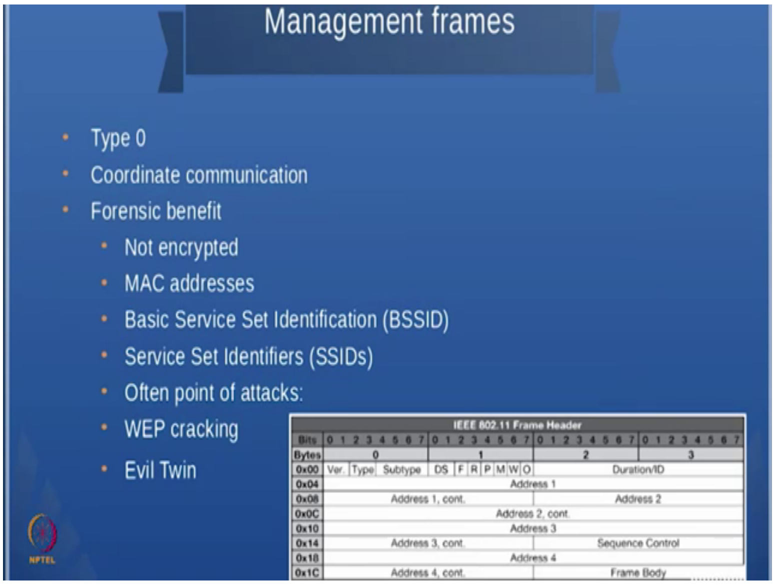


802.11 frame types

- Three types
  - Management Frames—Govern communications between stations, except flow control;
  - Control Frames—Support flow control over a variably available medium (such as RF);
  - Data Frames—Encapsulate the Layer 3+ data that moves between stations actively engaged in communication on a wireless network

Usually we will be concentrating more on 802.11 and 802.11 has three different frame types the first is the management frame, the control frame and the data frame. So, we should be aware of all the three frames, because when you are doing a forensic investigation or (Refer Time: 08:58) all these frames will matter ok. Management frames actually govern communication between two stations except the for the flow control and then control frames support flow control and then the data frames actually encapsulate the layer t data and it I mean the data frame is the one which actually move the data between stations on a wireless network ok.

(Refer Slide Time: 09:22)



## Management frames

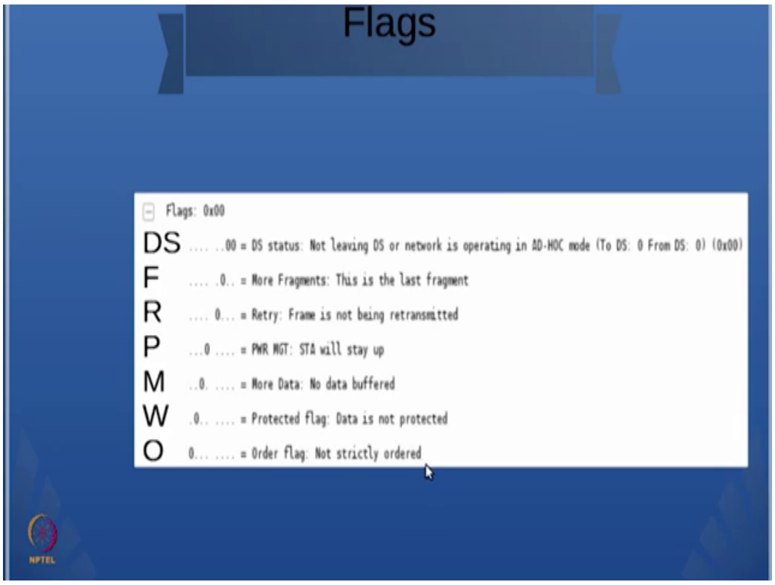
- Type 0
- Coordinate communication
- Forensic benefit
  - Not encrypted
  - MAC addresses
  - Basic Service Set Identification (BSSID)
  - Service Set Identifiers (SSIDs)
  - Often point of attacks:
  - WEP cracking
  - Evil Twin

IEEE 802.11 Frame Header

| Bits | 0 1 2 3 4 5 6 7 | 0 1 2 3 4 5 6 7 | 0 1 2 3 4 5 6 7 | 0 1 2 3 4 5 6 7 |
|---|---|---|---|---|
| Bytes | 0 | 1 | 2 | 3 |
| 0x00 | Ver. Type Subtype | DS F R P M W O | Duration/ID | |
| 0x04 | Address 1 | | | |
| 0x08 | Address 1, cont. | | Address 2 | |
| 0x0C | Address 2, cont. | | | |
| 0x10 | Address 3 | | | |
| 0x14 | Address 3, cont. | | Sequence Control | |
| 0x18 | Address 4 | | | |
| 0x1C | Address 4, cont. | | Frame Body | |

So, management frames are given as type 0 and these are the one to coordinate communication the forensic benefit of management frames is that its not encrypted it uses mac addresses. So, it uses BSSID you can get this service set identifiers and these are actually the point of attacks like evil twin attacks evil twin is using the same name for the wireless network connection as what is already existing; then you can crack you can crack you crack the web protocol the secret this frame looks something like this ok.

(Refer Slide Time: 10:11)



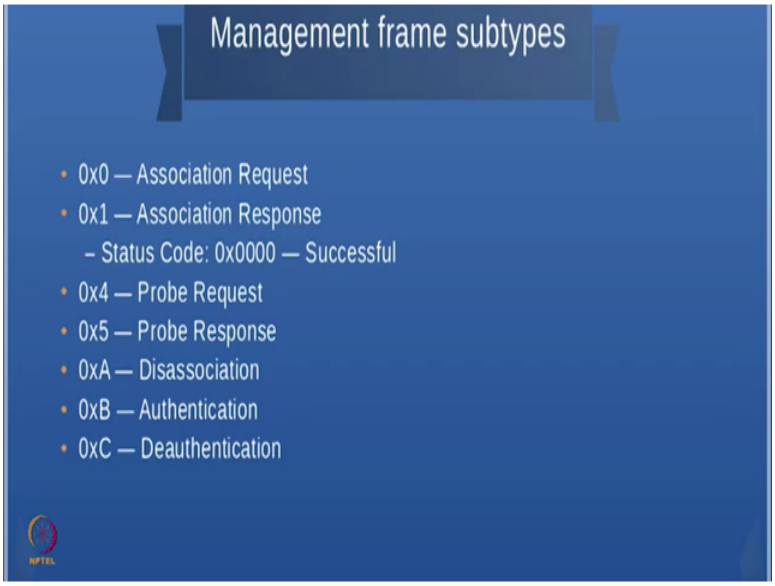
## Flags

```
⊟ Flags: 0x00
DS  .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
F   .... .0.. = More Fragments: This is the last fragment
R   .... 0... = Retry: Frame is not being retransmitted
P   ...0 .... = PWR MGT: STA will stay up
M   ..0. .... = More Data: No data buffered
W   .0.. .... = Protected flag: Data is not protected
O   0... .... = Order flag: Not strictly ordered
```

So, we will look at the I mean the you will have look at the flags I mean I mean you do not have to remember all these things, but you need to understand what these flags mean ok. So, for example, P P is equal to 0 means the power management flag and the idea is that usually your y shark will interpret it for you.

So, you need not remember all these things, but at least you should know; what is the value of each one of the field ok.

(Refer Slide Time: 10:39)



## Management frame subtypes

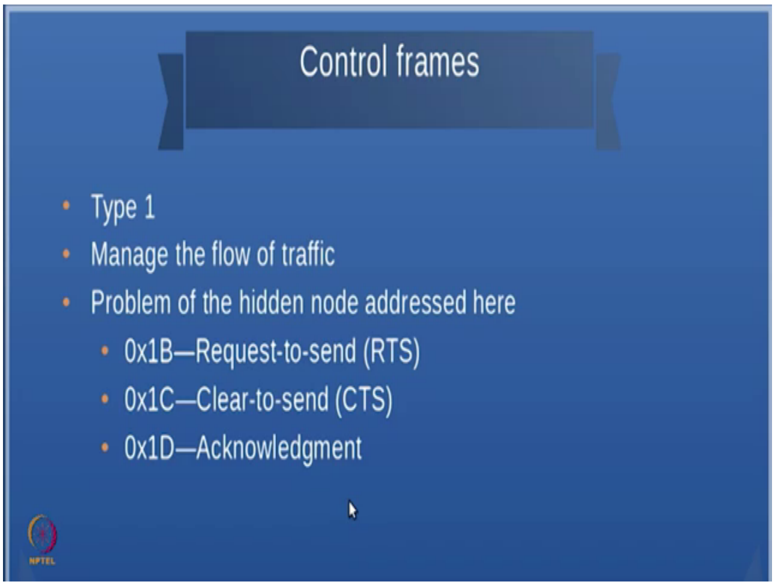
- 0x0 — Association Request
- 0x1 — Association Response
  - Status Code: 0x0000 — Successful
- 0x4 — Probe Request
- 0x5 — Probe Response
- 0xA — Disassociation
- 0xB — Authentication
- 0xC — Deauthentication

So, here are some management frame subtypes this is association request with a wireless network and then you get a response. So, all these code I mean you need not remember, but at least if you are using wire shark it will tell you whether its association request or association response, and if the if you are able to successfully connect it give it returns a successful connection and then the probe request is to find out what are all the wireless networks. I mean if you open a wireless network it tells you these are all the wireless networks that are available.

So, and then you have to you can associate with a particular wireless network and then you can disassociate sometimes these kind of hopping happens quite automatically for example, you could even have from a t 3G or a 4G network to a wireless network or wireless network to 4G network etcetera.

So, all that even between wireless networks from one wireless network to another wireless network ok.

(Refer Slide Time: 11:32)



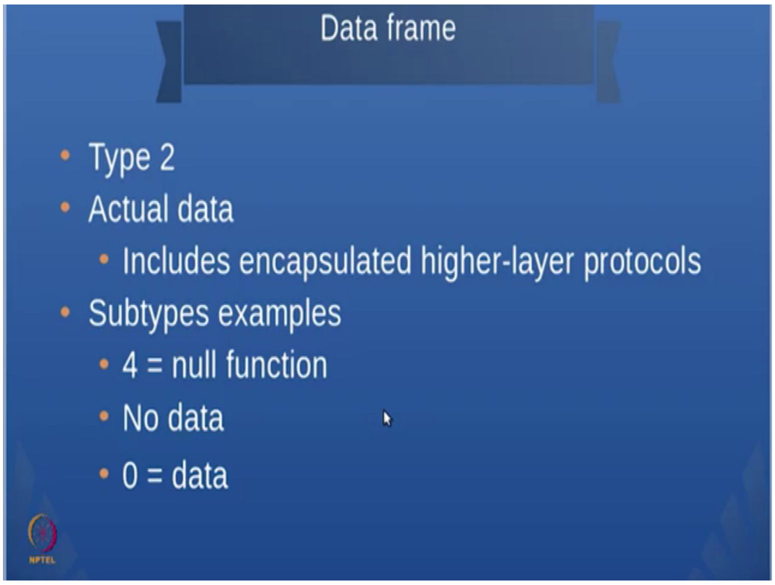
## Control frames

- Type 1
- Manage the flow of traffic
- Problem of the hidden node addressed here
  - 0x1B—Request-to-send (RTS)
  - 0x1C—Clear-to-send (CTS)
  - 0x1D—Acknowledgment

Then these control frames are type 1 frames. So, essentially it is similar to seat two sending and receiving data and model as a serial link for example, it has a request to send and clear to send those who have work with u arc will be very familiar with all these things anyway I mean this is a medium and you have to transfer data from one machine to another machine therefore, you are to have some sort of an acknowledgement to do flow control otherwise you will be barging in all the data and one of the things we need to have per flow control is because there is limited bandwidth in wireless networks.

So, because of that you or not everyone can go and congest the networks and if the network congestion happens that is drops and all these problems occur hope these were all covered in your previous IS courses. Then type two frame is the actual data frame it includes encapsulated higher level protocols ok.

(Refer Slide Time: 12:27)

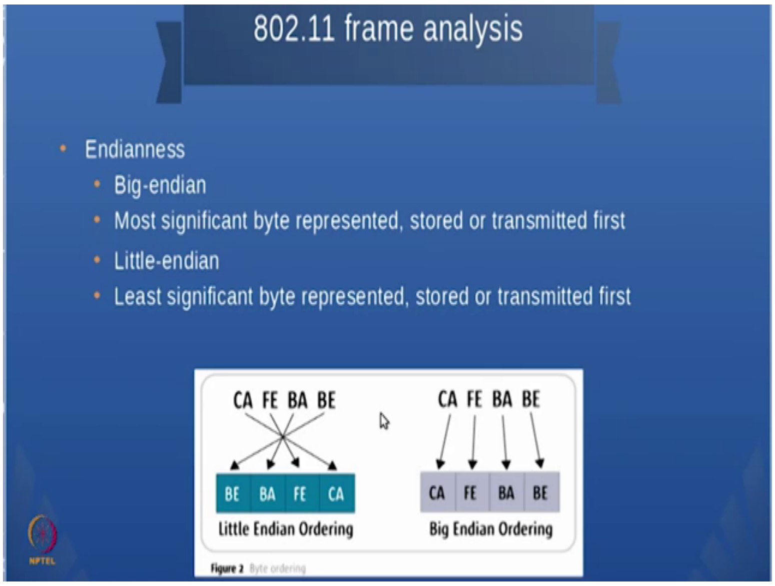


## Data frame

- Type 2
- Actual data
  - Includes encapsulated higher-layer protocols
- Subtypes examples
  - 4 = null function
  - No data
  - 0 = data

So, all the three frames type 0, type 1 and type 2 is of importance for a network forensic specialist ok.

(Refer Slide Time: 12:33)



## 802.11 frame analysis

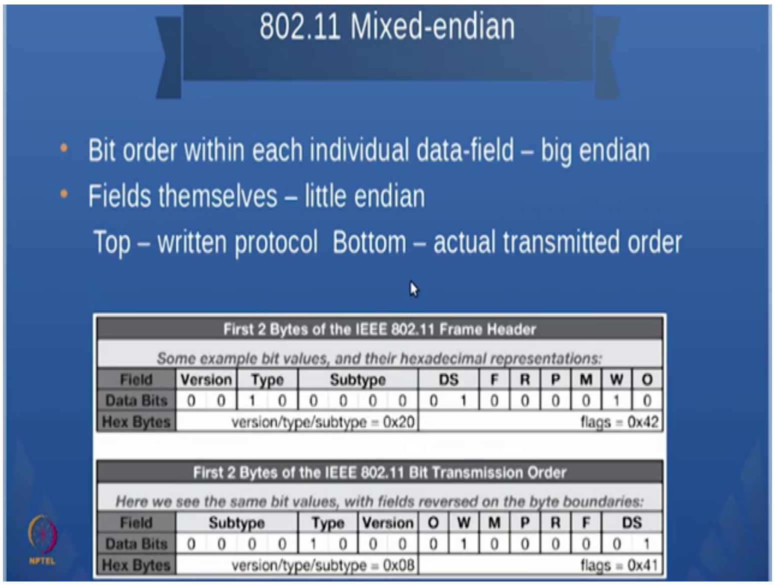
- Endianness
  - Big-endian
  - Most significant byte represented, stored or transmitted first
  - Little-endian
  - Least significant byte represented, stored or transmitted first

Figure 2 Byte ordering

So, while doing frame analysis you need to be careful about the endianness this was actually covered in your previous courses as network to host and host to network ok. So, it essentially big-endian means that the most significant byte represented or stored or transmitted first, but as little-endian is least significant byte represented stored or transmitted first ok.

So, if you look at this. So, sometimes what happens is that you could also have a mixed endian format ok.

(Refer Slide Time: 13:12)



## 802.11 Mixed-endian

- Bit order within each individual data-field – big endian
- Fields themselves – little endian

Top – written protocol  Bottom – actual transmitted order

First 2 Bytes of the IEEE 802.11 Frame Header

*Some example bit values, and their hexadecimal representations:*

| Field | Version | | Type | | Subtype | | | | DS | | F | R | P | M | W | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Data Bits | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| Hex Bytes | version/type/subtype = 0x20 | | | | | | | | flags = 0x42 | | | | | | | |

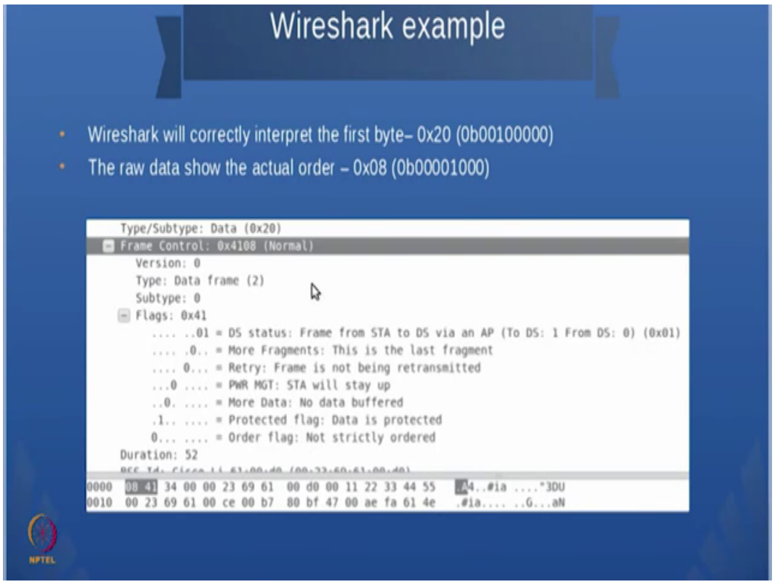
First 2 Bytes of the IEEE 802.11 Bit Transmission Order

*Here we see the same bit values, with fields reversed on the byte boundaries:*

| Field | Subtype | | | | Type | | Version | | O | W | M | P | R | F | DS | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Data Bits | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| Hex Bytes | version/type/subtype = 0x08 | | | | | | | | flags = 0x41 | | | | | | | |

So, here is an example ok. So, if you look at the first two bytes of IEEE 802.11 frame header you see 0 0 1 0 0 0 0 0 this is the way this is represented, but the way it gets transmitted is the other way around. So, if you look at this the subtype gets transmitted first, and then this type gets transmitted next and the version gets transmitted third.

(Refer Slide Time: 13:43)



## Wireshark example

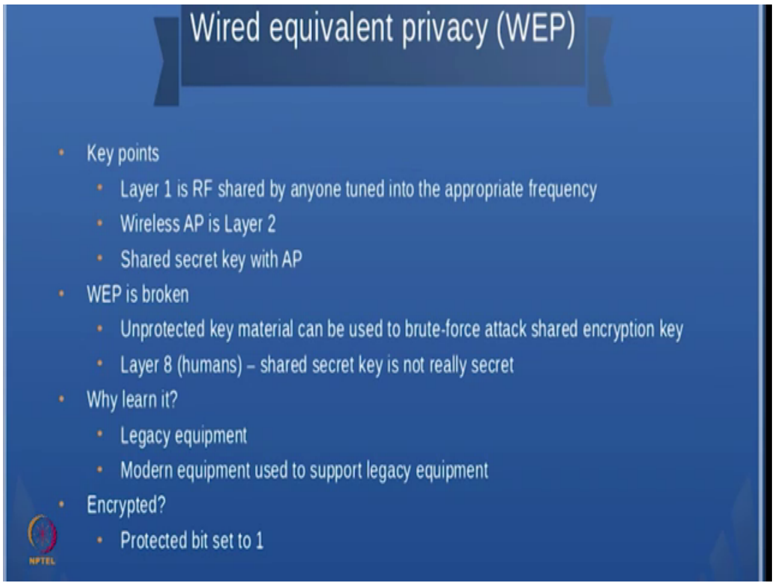
- Wireshark will correctly interpret the first byte– 0x20 (0b00100000)
- The raw data show the actual order – 0x08 (0b00001000)

```
    Type/Subtype: Data (0x20)
  ⊟ Frame Control: 0x4108 (Normal)
      Version: 0
      Type: Data frame (2)
      Subtype: 0
    ⊟ Flags: 0x41
        .... ..01 = DS status: Frame from STA to DS via an AP (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
        .1.. .... = Protected flag: Data is protected
        0... .... = Order flag: Not strictly ordered
    Duration: 52
0000  08 41 34 00 00 23 69 61  00 d0 00 11 22 33 44 55   .A4..#ia ....."3DU
0010  00 23 69 61 00 ce 00 b7  80 bf 47 00 ae fa 61 4e   .#ia.... ..G...aN
```

So, but you do not have to worry about it, because here is in wire shark you can just will correctly interpret these things ok. So, one of the things is yes you should be aware of this and if you look at the wire shark. So, it gives you all the information.

So, it talks about the frame control and then he talks about the version and it says that its a data frame then it looks at the flag and so, if you look at this ok. So, if you use wires hark you will be able to interpret all these frames correctly.

(Refer Slide Time: 14:15)



Wired equivalent privacy (WEP)

- Key points
  - Layer 1 is RF shared by anyone tuned into the appropriate frequency
  - Wireless AP is Layer 2
  - Shared secret key with AP
- WEP is broken
  - Unprotected key material can be used to brute-force attack shared encryption key
  - Layer 8 (humans) – shared secret key is not really secret
- Why learn it?
  - Legacy equipment
  - Modern equipment used to support legacy equipment
- Encrypted?
  - Protected bit set to 1

So, what we will do in the next module is that, we will look at wired equivalent privacy and why this used and why is there a security vulnerability, in wired equivalent privacy. And we will see how this is broken you can actually use a brute force attack to break this, why is it still used etcetera all these things we will see in the next module.

Thank you.