



Department of Electronic & Telecommunication Engineering

University of Moratuwa

EN3250 Internet of Things

Individual Assignment

2020 Batch - Semester 5

26/10/2023

200650U Thilakarathne D.L.J

Problem 1

- AP keeps transmitting beacons, and the Nokia mobile device(STA) uses Active scanning. STA instantiates probe requests. The AP responds to those probe requests with probe request responses. There are other devices as well, but we're focusing on these.
- STA send multiple probe requests and AP send multiple probe request responses as well.

No.	Time	Source	Destination	Protocol	Length	Info
686	43.725079	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=426, FN=0, Flags=....., BI=100, SSID="martine"
687	43.827482	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=427, FN=0, Flags=....., BI=100, SSID="martine"
688	43.929881	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=428, FN=0, Flags=....., BI=100, SSID="martine"
689	44.064860	NokiaDan_3d:aa:57	Broadcast	802.11	54	Probe Request, SN=4, FN=0, Flags=....., SSID="martinet3"
690	44.065518	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=430, FN=0, Flags=....., BI=100, SSID="martine"
691	44.066501	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=430, FN=0, Flags=....., BI=100, SSID="martine"
692	44.067957	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=430, FN=0, Flags=....., BI=100, SSID="martine"
693	44.071117	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=430, FN=0, Flags=....., BI=100, SSID="martine"
694	44.073657	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=430, FN=0, Flags=....., BI=100, SSID="martine"
695	44.076070	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=430, FN=0, Flags=....., BI=100, SSID="martine"
696	44.085663	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=430, FN=0, Flags=....., BI=100, SSID="martine"
697	44.134890	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=431, FN=0, Flags=....., BI=100, SSID="martine"
698	44.173685	NokiaDan_3d:aa:57	Broadcast	802.11	54	Probe Request, SN=7, FN=0, Flags=....., SSID="martinet3"
699	44.206260	NokiaDan_3d:aa:57	Broadcast	802.11	54	Probe Request, SN=8, FN=0, Flags=....., SSID="martinet3"
700	44.206922	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=432, FN=0, Flags=....., BI=100, SSID="martine"
701	44.207153	Siemens_41:bd:6e (00:01:e3:41:bd:6e) (RA)		802.11	10	Acknowledgement, Flags=.....
702	44.237074	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=433, FN=0, Flags=....., BI=100, SSID="martine"
703	44.314988	NokiaDan_3d:aa:57	Broadcast	802.11	54	Probe Request, SN=11, FN=0, Flags=....., SSID="martinet3"
704	44.339477	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=434, FN=0, Flags=....., BI=100, SSID="martine"
705	44.347636	NokiaDan_3d:aa:57	Broadcast	802.11	54	Probe Request, SN=12, FN=0, Flags=....., SSID="martinet3"
706	44.348282	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID="martine"
707	44.349370	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID="martine"
708	44.350295	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID="martine"
709	44.351210	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID="martine"
710	44.352609	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID="martine"
711	44.357027	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID="martine"
712	44.363487	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID="martine"
713	44.441864	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=436, FN=0, Flags=....., BI=100, SSID="martine"
714	44.544280	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=437, FN=0, Flags=....., BI=100, SSID="martine"
715	44.545208	NokiaDan_3d:aa:57	Siemens_41:bd:6e	802.11	30	Authentication. SN=13. FN=0. Flags=.....

But at one point STA enters the Authentication phase. The interchange of information between the AP and the STA, where each side proves the knowledge of a given password.

The screenshot shows a Wireshark capture of IEEE 802.11 frames. The display filter is 'nokia.pcap'. The packet list shows frames 704 through 733. The packet details pane for packet 712 (selected) shows an 'Authentication' frame (SN=13, FN=0, Flags=....., BI=100, SSID='martinet3'). The packet bytes pane shows the raw data of the authentication frame.

No.	Time	Source	Destination	Protocol	Length	Info
704	44.339477	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=434, FN=0, Flags=....., BI=100, SSID='martinet3'
705	44.347636	NokiaDan_3d:aa:57	Broadcast	802.11	54	Probe Request, SN=12, FN=0, Flags=....., SSID='martinet3'
706	44.348282	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
707	44.349370	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
708	44.350295	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
709	44.351210	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
710	44.352609	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
711	44.357027	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
712	44.363487	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
713	44.441864	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=436, FN=0, Flags=....., BI=100, SSID='martinet3'
714	44.544280	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=437, FN=0, Flags=....., BI=100, SSID='martinet3'
715	44.545208	NokiaDan_3d:aa:57	Siemens_41:bd:6e	802.11	30	Authentication, SN=13, FN=0, Flags=.....
716	44.545432	NokiaDan_3d:aa:57	NokiaDan_3d:aa:57 (00:16:bc:3d:aa:57) (RA)	802.11	10	Acknowledgement, Flags=.....
717	44.546099	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	38	Authentication, SN=438, FN=0, Flags=.....
718	44.546397	Siemens_41:bd:6e	Siemens_41:bd:6e (00:01:e3:41:bd:6e) (RA)	802.11	10	Acknowledgement, Flags=.....
719	44.547196	NokiaDan_3d:aa:57	Siemens_41:bd:6e	802.11	79	Association Request, SN=14, FN=0, Flags=....., SSID='martinet3'
720	44.547416	NokiaDan_3d:aa:57	NokiaDan_3d:aa:57 (00:16:bc:3d:aa:57) (RA)	802.11	10	Acknowledgement, Flags=.....
721	44.548462	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	54	Association Response, SN=439, FN=0, Flags=.....
722	44.548746	Siemens_41:bd:6e	Siemens_41:bd:6e (00:01:e3:41:bd:6e) (RA)	802.11	10	Acknowledgement, Flags=.....
723	44.549375	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
724	44.549556	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
725	44.549898	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
726	44.551575	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
727	44.551861	Siemens_41:bd:6e	Siemens_41:bd:6e (00:01:e3:41:bd:6e) (RA)	802.11	10	Acknowledgement, Flags=.....
728	44.589878	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
729	44.590291	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
730	44.590631	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
731	44.591095	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
732	44.591151	NokiaDan_3d:aa:57	NokiaDan_3d:aa:57 (00:16:bc:3d:aa:57) (RA)	802.11	10	Acknowledgement, Flags=.....
733	44.593409	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)

Then the device sends an association request frame to the AP.

The screenshot shows a Wireshark capture of IEEE 802.11 frames. The display filter is 'nokia.pcap'. The packet list shows frames 710 through 739. The packet details pane for packet 719 (selected) shows an 'Association Request' frame (SN=14, FN=0, Flags=....., SSID='martinet3'). The packet bytes pane shows the raw data of the association request frame.

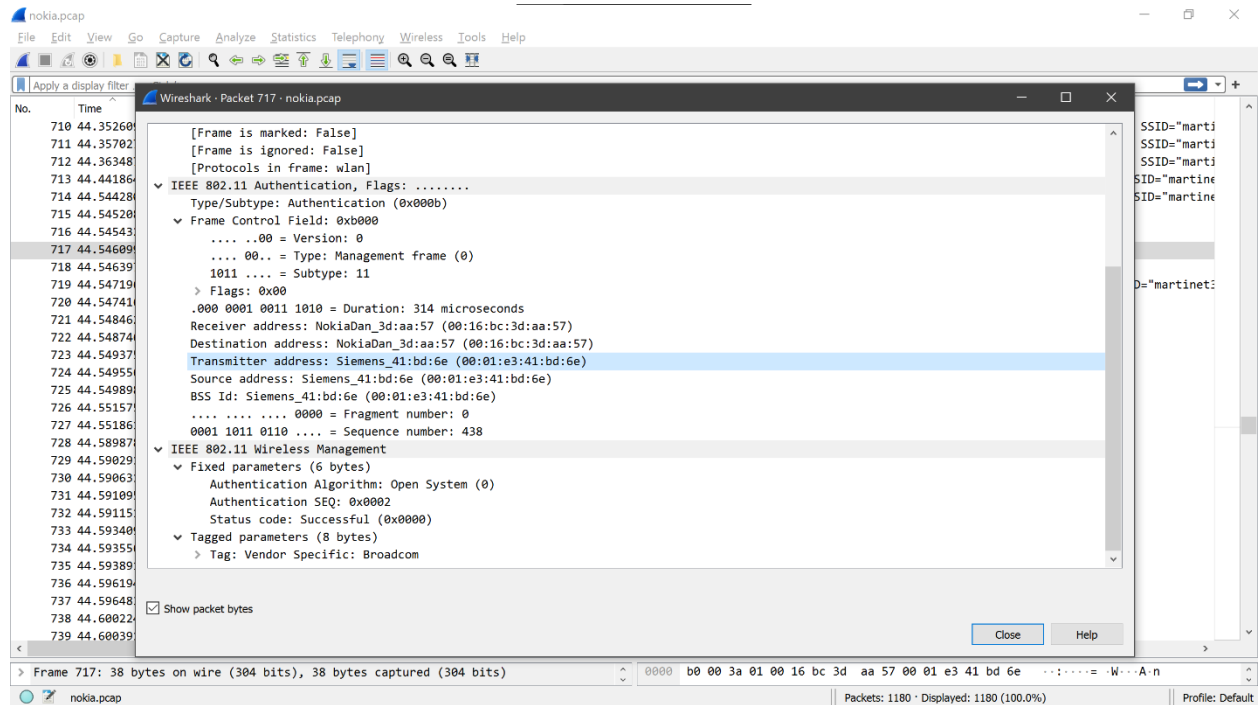
No.	Time	Source	Destination	Protocol	Length	Info
710	44.352609	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
711	44.357027	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
712	44.363487	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	104	Probe Response, SN=435, FN=0, Flags=....., BI=100, SSID='martinet3'
713	44.441864	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=436, FN=0, Flags=....., BI=100, SSID='martinet3'
714	44.544280	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=437, FN=0, Flags=....., BI=100, SSID='martinet3'
715	44.545208	NokiaDan_3d:aa:57	Siemens_41:bd:6e	802.11	30	Authentication, SN=13, FN=0, Flags=.....
716	44.545432	NokiaDan_3d:aa:57	NokiaDan_3d:aa:57 (00:16:bc:3d:aa:57) (RA)	802.11	10	Acknowledgement, Flags=.....
717	44.546099	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	38	Authentication, SN=438, FN=0, Flags=.....
718	44.546397	Siemens_41:bd:6e	Siemens_41:bd:6e (00:01:e3:41:bd:6e) (RA)	802.11	10	Acknowledgement, Flags=.....
719	44.547196	NokiaDan_3d:aa:57	Siemens_41:bd:6e	802.11	79	Association Request, SN=14, FN=0, Flags=....., SSID='martinet3'
720	44.547416	NokiaDan_3d:aa:57	NokiaDan_3d:aa:57 (00:16:bc:3d:aa:57) (RA)	802.11	10	Acknowledgement, Flags=.....
721	44.548462	Siemens_41:bd:6e	NokiaDan_3d:aa:57	802.11	54	Association Response, SN=439, FN=0, Flags=.....
722	44.548746	Siemens_41:bd:6e	Siemens_41:bd:6e (00:01:e3:41:bd:6e) (RA)	802.11	10	Acknowledgement, Flags=.....
723	44.549375	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
724	44.549556	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
725	44.549898	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
726	44.551575	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	131	Key (Message 1 of 4)
727	44.551861	Siemens_41:bd:6e	Siemens_41:bd:6e (00:01:e3:41:bd:6e) (RA)	802.11	10	Acknowledgement, Flags=.....
728	44.589878	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
729	44.590291	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
730	44.590631	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
731	44.591095	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	155	Key (Message 2 of 4)
732	44.591151	NokiaDan_3d:aa:57	NokiaDan_3d:aa:57 (00:16:bc:3d:aa:57) (RA)	802.11	10	Acknowledgement, Flags=.....
733	44.593409	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)
734	44.593556	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)
735	44.593891	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)
736	44.596194	Siemens_41:bd:6e	NokiaDan_3d:aa:57	EAPOL	155	Key (Message 3 of 4)
737	44.596483	Siemens_41:bd:6e	Siemens_41:bd:6e (00:01:e3:41:bd:6e) (RA)	802.11	10	Acknowledgement, Flags=.....
738	44.600224	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	131	Key (Message 4 of 4)
739	44.600391	NokiaDan_3d:aa:57	Siemens_41:bd:6e	EAPOL	131	Key (Message 4 of 4)

The AP subsequently reply with an association response frame that will allow the STA to join the network or be excluded. Then the STA is included, the AP releases an association ID to the client and add it to the list of connected clients. At this point, data can be exchanged with the AP and vice versa. All data frames will be followed by an acknowledgment.

- c) SSID: Siemens_41:bd:6e
BSSID: 00:01:e3:41:bd:6e

The pair (BSSID, SSID) found by any device at a particular location is called the “fingerprint” of that location.

This is unique to a given physical location, and hence a useful feature for localization.

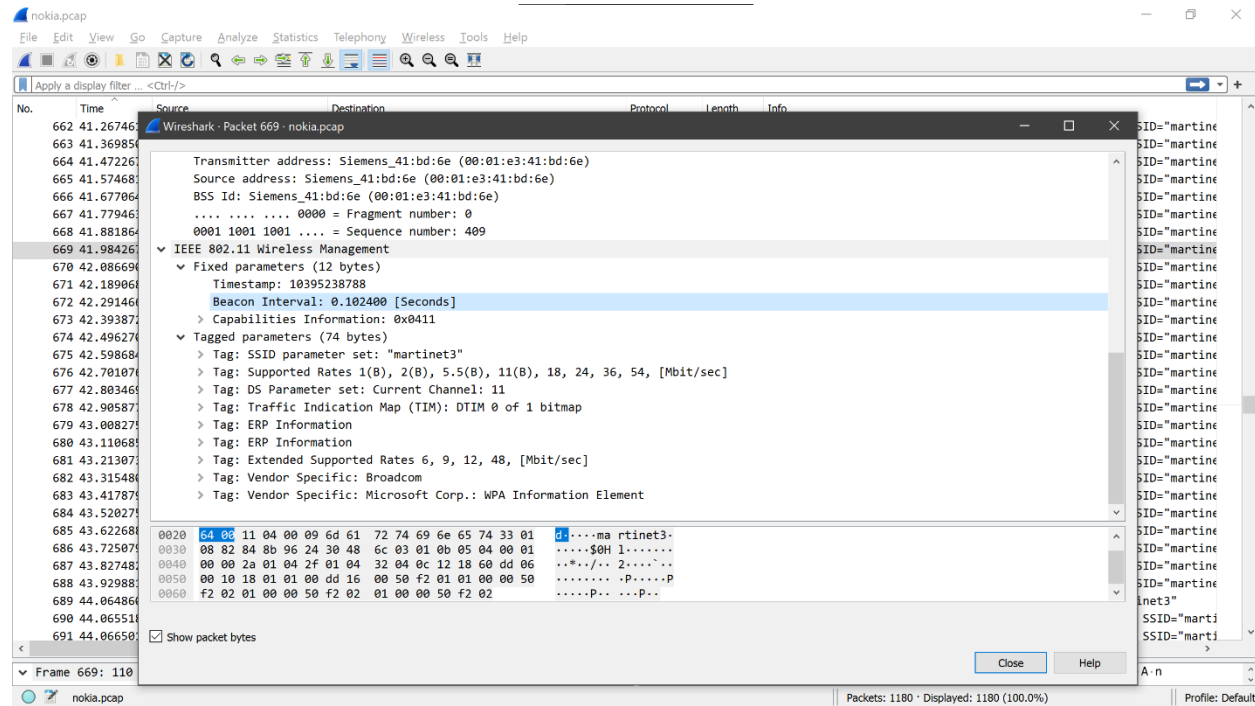


d) Passive scanning:

1. uses beacons and probe requests.
2. After a channel is selected, the device performing the scan will receive beacons and probe requests from nearby STAs.
3. An access point may transmit a beacon, and if the STA receives the transmission, it may progress to join the network.
4. This mode of scanning uses less power.

e)

1. By opening a captured beacon sent:



2. By checking the time interval between the beacon transmissions.

665	41.574681	Siemens_41:bd:6e	Broadcast
666	41.677064	Siemens_41:bd:6e	Broadcast
667	41.779463	Siemens_41:bd:6e	Broadcast
668	41.881864	Siemens_41:bd:6e	Broadcast
669	41.984267	Siemens_41:bd:6e	Broadcast
670	42.086690	Siemens_41:bd:6e	Broadcast
671	42.189068	Siemens_41:bd:6e	Broadcast
672	42.291466	Siemens_41:bd:6e	Broadcast
673	42.393872	Siemens_41:bd:6e	Broadcast
674	42.496270	Siemens_41:bd:6e	Broadcast

Calculation

$41.881864 - 41.779463 = 0.10240100000000 \text{ s}$

f)

	Source	Destination	Protocol	Length	Info
.267461	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=402, FN=0, Flag:
.369856	Wireshark · Packet 667 · nokia.pcap				
.472267					
.574681					
.677064	> Capabilities Information: 0x0411				
.779463	▼ Tagged parameters (74 bytes)				
.881864	> Tag: SSID parameter set: "martinet3"				
.984267	> Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]				
.086690	> Tag: DS Parameter set: Current Channel: 11				
.189068	> Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap				
.291466	> Tag: ERP Information				
.393872	> Tag: ERP Information				
.496270	> Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]				
.598684	> Tag: Vendor Specific: Broadcom				
.701076	> Tag: Vendor Specific: Microsoft Corp.: WPA Information Element				
.803469					
.905877	0000	80 00 00 00 ff ff ff ff ff ff 00 01 e3 41 bd 6e	A.n	
.005877	0010	00 01 e3 41 bd 6e 70 19 89 a1 97 6b 02 00 00 00	...A.np...	k...	
.008275	0020	64 00 11 04 00 09 6d 61 72 74 69 6e 65 74 33 01	d....ma	rtinet3.	
.110689	0030	08 82 84 8b 96 24 30 48 6c 03 01 0b 05 04 00 01\$0H l	
.213073	0040	00 00 2a 01 04 2f 01 04 32 04 0c 12 18 60 dd 06	..*./.. 2`..	
.315480	0050	00 10 18 01 01 00 dd 16 00 50 f2 01 01 00 00 50PP	
.417879	0060	f2 02 01 00 00 50 f2 02 01 00 00 50 f2 02P..	...P..	
.520275					
.622688					
.725075					
.827482					
.929881					
.064866					

Problem 2

a) For example,

Skip Time Resource:

This resource could be identified as `/.well-known/skip-time`. The skipping rope could expose the time duration of the skip in milliseconds through this resource. The endpoint could be something like,

`coap://<skipping_rope_IP>/.well-known/skip-time`.

Total Skip Number Resource:

This resource could be identified as `/.well-known/total-skip-number`. For instance, the skipping rope could expose the total count of skips through this resource. The endpoint could be something like,

`coap://<skipping_rope_IP>/.well-known/total-skip-number`.

Calories Burned Resource:

This resource could be identified as `/.well-known/calories-burned`. It could provide the number of calories burned during the skipping session. The endpoint could be something like,

`coap://<skipping_rope_IP>/.well-known/calories-burned`.

Tangles Resource:

This resource could be identified as `/.well-known/tangles`. It could indicate the number of times the rope has tangled during the session. The endpoint could be something like,

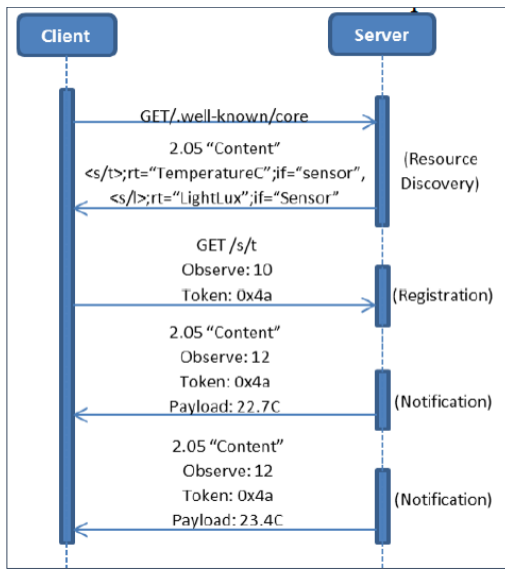
`coap://<skipping_rope_IP>/.well-known/tangles`.

Battery Level Resource:

This resource could be identified as `/.well-known/battery-level`. It could reveal the current battery level of the skipping rope. The endpoint could be something like,

`coap://<skipping_rope_IP>/.well-known/battery-level`.

b)



c) Advantages of using CoAP:

- Lightweight Protocol
- RESTful Interaction
- Efficiency in Small Data Transfers
- Less Complex Implementation

Disadvantages of using CoAP:

- Limited QoS Support
- Scalability Issues
- Limited Broker Functionality.
- Security Concerns

Problem 3

a)

- Machine usage
- Power usage
- Worker presence
- Machine Idle times/ efficiency
- Inventory updates/ Water tanks

b) Consider the Machine usage and Power usage

- Monitoring the power usage allows to avoid any failures, plant shutdown etc.
- Machine usage monitoring will allow to optimize the production line, reducing unwanted power consumption, produce more output etc.

c) The main challenge is that the production line must not stop while digitalization. The experts at TeeJay Lanka PLC showed that, they implemented the IOT devices parallel to the production line

d) _

e) The main factors would be the ROI.