

Scenario 1: Network Traffic Analysis

Task1.1:

ip.src == 192.168.60.1						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.010160	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[69]
6	10.008663	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[70]
8	13.584798	192.168.60.1	192.168.21.204	UDP	80	47889 - 3107 Len=38
10	18.635907	192.168.60.1	192.168.21.204	UDP	80	47889 - 3107 Len=38
12	20.69576	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[71]
14	30.693486	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[72]
17	35.5702219	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=20
19	35.536069	192.168.60.1	192.168.60.255	UDP	62	47889 - 47889 Len=20
20	35.536064	192.168.60.1	192.168.21.100	BACnet..	68	Unconfirmed-REQ i-Am device,33000
24	35.536095	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=26
22	35.543925	192.168.60.1	192.168.60.255	UDP	72	47889 - 47889 Len=30
24	35.559676	192.168.60.1	192.168.21.204	UDP	68	47889 - 3110 Len=26
25	35.570813	192.168.60.1	192.168.60.255	UDP	66	47889 - 47889 Len=24
26	35.574136	192.168.60.1	192.168.21.100	BACnet..	72	Unconfirmed-REQ i-Am device,33003
28	35.655817	192.168.60.1	192.168.60.255	UDP	60	47889 - 47889 Len=15
29	35.656467	192.168.60.1	192.168.60.255	UDP	60	47889 - 47889 Len=9
30	35.657739	192.168.60.1	192.168.21.100	BACnet..	60	I-Am-Router-To-Network
32	36.395151	192.168.60.1	192.168.21.204	UDP	88	47889 - 3110 Len=46
34	40.991356	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[73]
36	40.615641	192.168.60.1	192.168.21.204	UDP	68	47889 - 3110 Len=26
38	45.642728	192.168.60.1	192.168.21.204	UDP	68	47889 - 3110 Len=26
40	45.879459	192.168.60.1	192.168.21.204	UDP	80	47889 - 3110 Len=38
42	50.991697	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[74]
44	50.646381	192.168.60.1	192.168.21.204	UDP	68	47889 - 3110 Len=26
46	50.994916	192.168.60.1	192.168.21.204	UDP	80	47889 - 3110 Len=38
48	59.997923	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[75]
50	70.991329	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[76]
54	80.991945	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[77]
55	88.879649	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[235] loop,1 present-value
58	89.993325	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[78]
59	98.877133	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[236] loop,1 present-value
64	98.893137	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=18

ip.src == 192.168.60.1						
No.	Time	Source	Destination	Protocol	Length	Info
59	98.877133	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[236] loop,1 present-value
64	98.893137	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=18
65	98.899718	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=20
66	98.993075	192.168.60.1	192.168.21.100	BACnet..	68	Unconfirmed-REQ i-Am device,33000
67	98.998942	192.168.60.1	192.168.60.255	UDP	72	47889 - 47889 Len=30
69	98.915944	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=26
70	98.927643	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26
71	98.933968	192.168.60.1	192.168.60.255	UDP	66	47889 - 47889 Len=24
72	98.942878	192.168.60.1	192.168.21.100	BACnet..	72	Unconfirmed-REQ i-Am device,33003
74	99.617288	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=15
75	99.617858	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=9
76	99.619217	192.168.60.1	192.168.21.100	BACnet..	60	I-Am-Router-To-Network
78	99.691849	192.168.60.1	192.168.21.204	UDP	88	47889 - 3111 Len=46
88	99.93469	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[79]
82	103.974844	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26
85	103.993265	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=18
86	107.69393	192.168.60.1	192.168.60.255	UDP	62	47889 - 47889 Len=20
87	107.697250	192.168.60.1	192.168.21.100	BACnet..	68	Unconfirmed-REQ i-Am device,33000
88	107.700125	192.168.60.1	192.168.60.255	UDP	68	47889 - 47889 Len=26
99	107.716913	192.168.60.1	192.168.60.255	UDP	72	47889 - 47889 Len=30
91	107.730871	192.168.60.1	192.168.60.255	UDP	66	47889 - 47889 Len=24
92	107.732335	192.168.60.1	192.168.21.100	BACnet..	72	Unconfirmed-REQ i-Am device,33003
94	107.774745	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26
96	107.993435	192.168.60.1	192.168.21.204	UDP	72	47889 - 3111 Len=30
98	108.495640	192.168.60.1	192.168.21.204	UDP	143	47889 - 3111 Len=101
100	108.705614	192.168.60.1	192.168.21.204	UDP	71	47889 - 3111 Len=29
102	108.797264	192.168.60.1	192.168.21.204	UDP	88	47889 - 3111 Len=46
104	108.873952	192.168.60.1	192.168.21.100	BACnet..	68	Confirmed-REQ readProperty[237] loop,1 present-value
106	108.888244	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26
109	108.991473	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26
110	109.619586	192.168.60.1	192.168.21.204	UDP	113	47889 - 3111 Len=71
112	109.112256	192.168.60.1	192.168.21.204	UDP	91	47889 - 3111 Len=49
114	109.114620	192.168.60.1	192.168.21.204	UDP	91	47889 - 3111 Len=49
116	109.989646	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[80]
119	112.796587	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26
121	113.638160	192.168.60.1	192.168.21.204	UDP	80	47889 - 3111 Len=38
123	114.690280	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26
125	117.832244	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26
127	118.695618	192.168.60.1	192.168.21.204	UDP	88	47889 - 3111 Len=38
128	118.872447	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[238] loop,1 present-value
131	119.990254	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[81]
133	122.889188	192.168.60.1	192.168.21.204	UDP	68	47889 - 3111 Len=26

Task1.2:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[69]
5	9.998947	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[70]
7	13.573216	192.168.21.204	192.168.60.1	UDP	60	3107 ~ 47809 Len=17
9	18.623781	192.168.21.204	192.168.60.1	UDP	60	3107 ~ 47809 Len=17
11	19.996931	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[71]
13	29.995796	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[72]
15	35.527173	192.168.21.100	192.168.60.1	BACNet...	60	Unconfirmed-REQ who-Is
16	35.530619	192.168.21.100	192.168.60.1	BACNet...	60	Unconfirmed-REQ i-Am-device, 35200
19	35.535427	192.168.21.100	192.168.60.1	BACNet...	72	Unconfirmed-REQ i-Am-device, 3535
23	35.553898	192.168.21.204	192.168.60.1	UDP	60	3110 ~ 47809 Len=17
27	35.652383	192.168.21.100	192.168.60.1	BACNet...	60	Who-Is-Router-To-Network
31	36.350887	192.168.21.204	192.168.60.1	UDP	76	3110 ~ 47809 Len=28
33	39.994064	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[73]
35	40.669711	192.168.21.204	192.168.60.1	UDP	60	3110 ~ 47809 Len=17
37	45.633899	192.168.21.204	192.168.60.1	UDP	60	3110 ~ 47809 Len=17
39	45.861483	192.168.21.204	192.168.60.1	UDP	60	3110 ~ 47809 Len=17
41	49.993316	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[74]
43	50.649973	192.168.21.204	192.168.60.1	UDP	60	3110 ~ 47809 Len=17
45	50.893968	192.168.21.204	192.168.60.1	UDP	60	3110 ~ 47809 Len=17
47	59.991313	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[75]
49	69.996142	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[76]
53	79.988667	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[77]
56	88.882514	192.168.21.100	192.168.60.1	BACNet...	65	Complex-ACK readProperty[235] loop,1 present-value
57	89.987893	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[78]
66	98.886793	192.168.21.100	192.168.60.1	BACNet...	60	Unconfirmed-REQ who-Is
61	98.882169	192.168.21.100	192.168.60.1	BACNet...	72	Unconfirmed-REQ i-Am-device, 3535
62	98.884767	192.168.21.100	192.168.60.1	BACNet...	65	Complex-ACK readProperty[236] loop,1 present-value
63	98.887789	192.168.21.100	192.168.60.1	BACNet...	68	Unconfirmed-REQ i-Am-device, 35200
66	98.912331	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
73	99.813084	192.168.21.100	192.168.60.1	BACNet...	60	Who-Is-Router-To-Network
77	99.619898	192.168.21.204	192.168.60.1	UDP	76	3111 ~ 47809 Len=28
79	99.985898	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[79]
81	103.966677	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
83	107.667653	192.168.21.100	192.168.60.1	BACNet...	60	Unconfirmed-REQ who-Is
84	107.699662	192.168.21.100	192.168.60.1	BACNet...	68	Unconfirmed-REQ i-Am-device, 35200
89	107.713841	192.168.21.100	192.168.60.1	BACNet...	72	Unconfirmed-REQ i-Am-device, 3535
93	107.764235	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
95	107.963437	192.168.21.204	192.168.60.1	UDP	64	3111 ~ 47809 Len=22
97	108.363834	192.168.21.204	192.168.60.1	UDP	76	3111 ~ 47809 Len=34
99	108.664371	192.168.21.204	192.168.60.1	UDP	70	3111 ~ 47809 Len=28
101	108.764480	192.168.21.204	192.168.60.1	UDP	70	3111 ~ 47809 Len=28
103	108.864426	192.168.21.204	192.168.60.1	UDP	66	3111 ~ 47809 Len=24
105	108.876674	192.168.21.100	192.168.60.1	BACNet...	65	Complex-ACK readProperty[237] loop,1 present-value
107	108.964756	192.168.21.204	192.168.60.1	UDP	70	3111 ~ 47809 Len=28
108	108.998335	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
111	109.664899	192.168.21.204	192.168.60.1	UDP	70	3111 ~ 47809 Len=28
113	109.105122	192.168.21.204	192.168.60.1	UDP	71	3111 ~ 47809 Len=29
115	109.994236	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[80]
118	122.779308	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
120	123.622655	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
122	123.999958	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
124	127.828261	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
126	128.678445	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17
129	128.875529	192.168.21.100	192.168.60.1	BACNet...	65	Complex-ACK readProperty[238] loop,1 present-value
130	129.992898	192.168.21.100	192.168.60.1	BACNet...	61	Confirmed-REQ readPropertyMultiple[81]
132	122.873464	192.168.21.204	192.168.60.1	UDP	60	3111 ~ 47809 Len=17

Task1.3:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[69]
2	0.010160	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[69]
5	9.998947	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[70]
6	10.008663	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[70]
7	13.573216	192.168.21.204	192.168.60.1	UDP	60	3107 - 47809 Len=17
8	13.584798	192.168.60.1	192.168.21.204	UDP	88	47809 - 3107 Len=38
9	18.623781	192.168.21.204	192.168.60.1	UDP	60	3107 - 47809 Len=17
10	18.633597	192.168.60.1	192.168.21.204	UDP	88	47809 - 3107 Len=38
11	19.996931	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[71]
12	19.997676	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[71]
13	29.895796	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[72]
14	30.893486	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[72]
15	35.527173	192.168.21.100	192.168.60.1	BACnet..	60	Unconfirmed-REQ who-is
16	35.530814	192.168.21.100	192.168.60.1	BACnet..	68	Unconfirmed-REQ i-Am device,35200
17	35.532925	192.168.60.1	192.168.21.205	UDP	60	47809 - 47809 Len=18
18	35.535356	192.168.60.1	192.168.60.255	UDP	62	47809 - 47809 Len=20
19	35.535427	192.168.21.100	192.168.60.1	BACnet..	72	Unconfirmed-REQ i-Am device,3535
20	35.536664	192.168.60.1	192.168.21.100	BACnet..	68	Unconfirmed-REQ i-Am device,33000
21	35.539385	192.168.60.1	192.168.60.255	UDP	60	47809 - 47809 Len=26
22	35.543925	192.168.60.1	192.168.60.255	UDP	72	47809 - 47809 Len=30
23	35.553898	192.168.21.204	192.168.60.1	UDP	60	3110 - 47809 Len=17
24	35.559676	192.168.60.1	192.168.21.204	UDP	68	47809 - 3110 Len=26
25	35.570813	192.168.60.1	192.168.60.255	UDP	60	47809 - 47809 Len=24
26	35.574136	192.168.60.1	192.168.21.100	BACnet..	72	Unconfirmed-REQ i-Am device,33003
27	35.652383	192.168.21.100	192.168.60.1	BACnet..	68	Who-Is-Router-To-Network
28	35.655817	192.168.60.1	192.168.60.255	UDP	60	47809 - 47809 Len=15
29	35.656467	192.168.60.1	192.168.60.255	UDP	60	47809 - 47809 Len=9
30	35.657739	192.168.60.1	192.168.21.100	BACnet..	60	I-Am-Router-To-Network
31	36.350887	192.168.21.204	192.168.60.1	UDP	70	3110 - 47809 Len=28
32	36.395151	192.168.60.1	192.168.21.204	UDP	88	47809 - 3110 Len=46
33	39.994964	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[73]
34	40.001356	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[73]
35	40.606711	192.168.21.204	192.168.60.1	UDP	60	3110 - 47809 Len=17
<hr/>						
No.	Time	Source	Destination	Protocol	Length	Info
35	40.666711	192.168.21.204	192.168.60.1	UDP	60	3110 - 47809 Len=17
36	40.615641	192.168.60.1	192.168.21.204	UDP	68	47809 - 3110 Len=26
37	45.633869	192.168.21.204	192.168.60.1	UDP	60	3110 - 47809 Len=17
38	45.634228	192.168.60.1	192.168.21.204	UDP	68	47809 - 3110 Len=26
39	45.664103	192.168.21.204	192.168.60.1	UDP	60	3110 - 47809 Len=17
40	45.679459	192.168.60.1	192.168.21.204	UDP	88	47809 - 3110 Len=38
41	49.093316	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[74]
42	50.091957	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[74]
43	50.649973	192.168.21.204	192.168.60.1	UDP	60	3110 - 47809 Len=17
44	50.646381	192.168.60.1	192.168.21.204	UDP	68	47809 - 3110 Len=26
45	50.893068	192.168.21.204	192.168.60.1	UDP	60	3110 - 47809 Len=17
46	50.964916	192.168.60.1	192.168.21.204	UDP	88	47809 - 3110 Len=38
47	59.991313	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[75]
48	59.997923	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[75]
49	69.999142	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[76]
50	70.001329	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[76]
53	79.988607	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[77]
54	80.001645	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[77]
55	88.879649	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[235] loop,1 present-value
56	88.882514	192.168.21.100	192.168.60.1	BACnet..	65	Complex-ACK readProperty[235] loop,1 present-value
57	89.987089	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[78]
58	89.993325	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[78]
59	89.877133	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[236] loop,1 present-value
60	98.880793	192.168.21.100	192.168.60.1	BACnet..	60	Unconfirmed-REQ who-is
61	98.882169	192.168.21.100	192.168.60.1	BACnet..	72	Unconfirmed-REQ i-Am device,3535
62	98.884767	192.168.21.100	192.168.60.1	BACnet..	65	Complex-ACK readProperty[236] loop,1 present-value
63	98.887789	192.168.21.100	192.168.60.1	BACnet..	68	Unconfirmed-REQ i-Am device,35200
64	98.893137	192.168.60.1	192.168.60.255	UDP	60	47809 - 47809 Len=18
65	98.893718	192.168.60.1	192.168.60.255	UDP	62	47809 - 47809 Len=20
66	98.893875	192.168.60.1	192.168.21.100	BACnet..	60	Unconfirmed-REQ i-Am device,33000
67	98.893942	192.168.60.1	192.168.60.255	UDP	72	47809 - 47809 Len=38
68	98.912331	192.168.60.1	192.168.60.1	UDP	60	3110 - 47809 Len=17
69	98.915644	192.168.60.1	192.168.60.255	UDP	68	47809 - 47809 Len=26

No.	Time	Source	Destination	Protocol	Length	Info
69	98.915944	192.168.60.1	192.168.60.255	UDP	68	47809 → 47809 Len=26
70	98.927643	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26
71	98.939368	192.168.60.1	192.168.60.255	UDP	66	47809 → 47809 Len=24
72	98.942878	192.168.60.1	192.168.21.100	BACnet...	72	Unconfirmed-REQ i-Am device, 33003
73	99.613084	192.168.21.100	192.168.60.1	BACnet...	60	Who-Is-Router-To-Network
74	99.617200	192.168.60.1	192.168.60.255	UDP	68	47809 → 47809 Len=15
75	99.617859	192.168.60.1	192.168.60.255	UDP	68	47809 → 47809 Len=9
76	99.619217	192.168.60.1	192.168.21.100	BACnet...	66	I-Am-Router-To-Network
77	99.619889	192.168.21.204	192.168.60.1	UDP	70	3111 → 47809 Len=28
78	99.621849	192.168.60.1	192.168.21.204	UDP	80	47809 → 3111 Len=46
79	99.628906	192.168.21.100	192.168.60.1	BACnet...	67	Confirmed-REQ readPropertyMultiple[79]
80	99.629469	192.168.60.1	192.168.21.100	BACnet...	67	Complex-ACK readPropertyMultiple[79]
81	103.966677	192.168.21.204	192.168.60.1	UDP	60	3111 → 47809 Len=17
82	103.974844	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26
83	107.687653	192.168.21.100	192.168.60.1	BACnet...	60	Unconfirmed-REQ who-Is
84	107.690062	192.168.21.100	192.168.60.1	BACnet...	60	Unconfirmed-REQ i-Am device, 35200
85	107.692265	192.168.60.1	192.168.60.255	UDP	68	47809 → 47809 Len=18
86	107.696103	192.168.60.1	192.168.60.255	UDP	62	47809 → 47809 Len=20
87	107.697250	192.168.60.1	192.168.21.100	BACnet...	68	Unconfirmed-REQ i-Am device, 33000
88	107.700125	192.168.60.1	192.168.60.255	UDP	68	47809 → 47809 Len=26
89	107.708101	192.168.21.100	192.168.60.1	BACnet...	72	Unconfirmed-REQ i-Am device, 3535
90	107.716913	192.168.60.1	192.168.60.255	UDP	72	47809 → 47809 Len=30
91	107.730871	192.168.60.1	192.168.60.255	UDP	66	47809 → 47809 Len=24
92	107.732335	192.168.60.1	192.168.21.100	BACnet...	72	Unconfirmed-REQ i-Am device, 33003
93	107.764235	192.168.21.204	192.168.60.1	UDP	60	3111 → 47809 Len=17
94	107.774745	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26
95	107.963437	192.168.21.204	192.168.60.1	UDP	64	3111 → 47809 Len=22
96	107.993435	192.168.60.1	192.168.21.204	UDP	72	47809 → 3111 Len=30
97	108.363834	192.168.21.204	192.168.60.1	UDP	76	3111 → 47809 Len=34
98	108.405640	192.168.60.1	192.168.21.204	UDP	143	47809 → 3111 Len=101
99	108.664371	192.168.21.204	192.168.60.1	UDP	70	3111 → 47809 Len=28
100	108.705914	192.168.60.1	192.168.21.204	UDP	71	47809 → 3111 Len=29
101	108.705914	192.168.21.204	192.168.60.1	UDP	79	3111 → 47809 Len=28

No.	Time	Source	Destination	Protocol	Length	Info
101	108.764480	192.168.21.204	192.168.60.1	UDP	70	47809 → 47809 Len=28
102	108.797264	192.168.60.1	192.168.21.204	UDP	88	47809 → 3111 Len=46
103	108.864426	192.168.21.204	192.168.60.1	UDP	66	3111 → 47809 Len=24
104	108.873952	192.168.60.1	192.168.21.100	BACnet...	60	Confirmed-REQ readProperty[237] loop,1 present-value
105	108.876674	192.168.21.100	192.168.60.1	BACnet...	65	Complex-ACK readProperty[237] loop,1 present-value
106	108.888244	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26
107	108.964750	192.168.21.204	192.168.60.1	UDP	70	3111 → 47809 Len=28
108	108.983835	192.168.21.204	192.168.60.1	UDP	66	3111 → 47809 Len=17
109	108.991473	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26
110	109.019586	192.168.60.1	192.168.21.204	UDP	113	47809 → 3111 Len=71
111	109.060050	192.168.21.204	192.168.60.1	UDP	70	3111 → 47809 Len=28
112	109.147258	192.168.60.1	192.168.21.204	UDP	91	47809 → 3111 Len=39
113	109.165122	192.168.21.204	192.168.60.1	UDP	71	3111 → 47809 Len=29
114	109.264938	192.168.60.1	192.168.21.204	UDP	79	47809 → 3111 Len=28
115	109.984236	192.168.21.100	192.168.60.1	BACnet...	61	Confirmed-REQ readPropertyMultiple[80]
116	109.989646	192.168.60.1	192.168.21.100	BACnet...	67	Complex-ACK readPropertyMultiple[80]
117	110.789308	192.168.21.204	192.168.60.1	UDP	60	3111 → 47809 Len=17
119	112.796597	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26
120	113.626554	192.168.21.204	192.168.60.1	UDP	69	3111 → 47809 Len=17
121	113.636160	192.168.60.1	192.168.21.204	UDP	80	47809 → 3111 Len=38
122	113.989958	192.168.21.204	192.168.60.1	UDP	66	3111 → 47809 Len=17
123	114.690280	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26
124	117.828201	192.168.21.204	192.168.60.1	UDP	60	3111 → 47809 Len=17
125	117.832244	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26
126	118.678445	192.168.21.204	192.168.60.1	UDP	60	3111 → 47809 Len=17
127	118.695618	192.168.60.1	192.168.21.204	UDP	80	47809 → 3111 Len=38
128	118.872447	192.168.60.1	192.168.21.100	BACnet...	60	Confirmed-REQ readProperty[238] loop,1 present-value
129	118.875520	192.168.21.100	192.168.60.1	BACnet...	65	Complex-ACK readProperty[238] loop,1 present-value
130	119.982988	192.168.21.100	192.168.60.1	BACnet...	61	Confirmed-REQ readPropertyMultiple[81]
131	119.990254	192.168.60.1	192.168.21.100	BACnet...	67	Complex-ACK readPropertyMultiple[81]
132	122.873464	192.168.21.204	192.168.60.1	UDP	68	3111 → 47809 Len=17
133	122.889198	192.168.60.1	192.168.21.204	UDP	68	47809 → 3111 Len=26

Task1.4:

(ip.addr == 192.168.60.1 && ip.addr == 192.168.21.100) (ip.addr == 192.168.21.100 && ip.addr == 192.168.60.1)						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[69]
2	0.010160	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[69]
5	9.998947	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[70]
6	10.008603	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[70]
11	19.996931	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[71]
12	20.005676	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[71]
13	29.995796	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[72]
14	30.003486	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[72]
15	35.527173	192.168.21.100	192.168.60.1	BACnet..	69	Unconfirmed-REQ who-Is
16	35.530814	192.168.21.100	192.168.60.1	BACnet..	68	Unconfirmed-REQ i-Am device,35200
19	35.535427	192.168.21.100	192.168.60.1	BACnet..	72	Unconfirmed-REQ i-Am device,3535
20	35.536694	192.168.60.1	192.168.21.100	BACnet..	68	Unconfirmed-REQ i-Am device,33000
26	35.574136	192.168.60.1	192.168.21.100	BACnet..	72	Unconfirmed-REQ i-Am device,33003
27	35.652983	192.168.21.100	192.168.60.1	BACnet..	68	Who-Is-Router-To-Network
30	35.657739	192.168.60.1	192.168.21.100	BACnet..	68	I-Am-Router-To-Network
33	35.661444	192.168.60.1	192.168.21.100	BACnet..	61	Confirmed-REQ readPropertyMultiple[73]
34	40.001356	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[73]
41	49.993316	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[74]
42	50.001697	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[74]
47	59.991313	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[75]
48	59.997923	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[75]
49	69.990142	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[76]
50	70.001329	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[76]
53	79.988667	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[77]
54	80.001845	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[77]
55	88.879649	192.168.60.1	192.168.21.100	BACnet..	68	Confirmed-REQ readProperty[235] loop,1 present-value
56	88.882514	192.168.21.100	192.168.60.1	BACnet..	65	Complex-ACK readProperty[235] loop,1 present-value
57	89.987089	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[78]
58	89.993325	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[78]
59	89.977133	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readPropertyMultiple[78]
60	98.877133	192.168.60.1	192.168.21.100	BACnet..	68	Confirmed-REQ readProperty[236] loop,1 present-value
61	98.882169	192.168.21.100	192.168.60.1	BACnet..	72	Unconfirmed-REQ i-Am device,3535
62	98.884767	192.168.21.100	192.168.60.1	BACnet..	65	Complex-ACK readProperty[236] loop,1 present-value
(ip.addr == 192.168.60.1 && ip.addr == 192.168.21.100) (ip.addr == 192.168.21.100 && ip.addr == 192.168.60.1)						
No.	Time	Source	Destination	Protocol	Length	Info
49	69.990142	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[76]
50	70.001329	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[76]
53	79.988667	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[77]
54	80.001045	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[77]
55	88.879649	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[238] loop,1 present-value
56	88.882514	192.168.21.100	192.168.60.1	BACnet..	65	Complex-ACK readProperty[238] loop,1 present-value
57	89.987089	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[78]
58	89.993325	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[78]
59	89.977133	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readPropertyMultiple[78]
60	98.877133	192.168.60.1	192.168.21.100	BACnet..	68	Confirmed-REQ readProperty[236] loop,1 present-value
61	98.882169	192.168.21.100	192.168.60.1	BACnet..	72	Unconfirmed-REQ who-Is
62	98.884767	192.168.21.100	192.168.60.1	BACnet..	65	Complex-ACK readProperty[236] loop,1 present-value
63	98.887789	192.168.21.100	192.168.60.1	BACnet..	68	Unconfirmed-REQ i-Am device,3535
66	98.993075	192.168.60.1	192.168.21.100	BACnet..	68	Unconfirmed-REQ i-Am device,33000
72	98.942878	192.168.60.1	192.168.21.100	BACnet..	72	Unconfirmed-REQ i-Am device,33003
73	99.013084	192.168.21.100	192.168.60.1	BACnet..	60	Who-Is-Router-To-Network
76	99.019217	192.168.60.1	192.168.21.100	BACnet..	60	I-Am-Router-To-Network
79	99.985888	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[79]
80	99.993469	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[79]
83	107.667653	192.168.21.100	192.168.60.1	BACnet..	60	Unconfirmed-REQ who-Is
84	107.690062	192.168.21.100	192.168.60.1	BACnet..	68	Unconfirmed-REQ i-Am device,35200
87	107.697250	192.168.60.1	192.168.21.100	BACnet..	68	Unconfirmed-REQ i-Am device,35200
89	107.713841	192.168.21.100	192.168.60.1	BACnet..	72	Unconfirmed-REQ i-Am device,3535
92	107.732335	192.168.60.1	192.168.21.100	BACnet..	72	Unconfirmed-REQ i-Am device,33003
104	108.873952	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[237] loop,1 present-value
105	108.876674	192.168.21.100	192.168.60.1	BACnet..	65	Complex-ACK readProperty[237] loop,1 present-value
115	109.984236	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[80]
116	109.989646	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[80]
128	118.872447	192.168.60.1	192.168.21.100	BACnet..	60	Confirmed-REQ readProperty[238] loop,1 present-value
129	118.875529	192.168.21.100	192.168.60.1	BACnet..	65	Complex-ACK readProperty[238] loop,1 present-value
138	119.982989	192.168.21.100	192.168.60.1	BACnet..	61	Confirmed-REQ readPropertyMultiple[81]
131	119.990254	192.168.60.1	192.168.21.100	BACnet..	67	Complex-ACK readPropertyMultiple[81]

Scenario 2- VoIP Security Analysis

Task2.1:

Typical VoIP challenges encompass:

- Network Congestion: Elevated network activity causing a decline in call quality or interruptions.
- Jitter and Latency: Irregular arrival times of data packets causing audio quality issues.

- Packet Loss: Absence of transmitted packets leading to call drops or subpar audio quality.
- Codec Mismatch: Inconsistency between codecs potentially causing audio problems.

Issue Identified in this Situation:

Recurring call drops indicate potential problems related to network congestion, packet loss, or jitter.

Task2.2:

Only 6 packets as shown in the bottom right of the screen shot Packets: 412 Displayed: 6(1.6%)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.4	5.135.179.50	SIP/SDP	940	Request: INVITE sip:test@startrinity.com
2	0.367477	5.135.179.50	192.168.10.4	SIP	399	Status: 100 Trying
3	2.285223	5.135.179.50	192.168.10.4	SIP/SDP	924	Status: 200 OK (INVITE)
4	2.290395	192.168.10.4	5.135.179.50	SIP	412	Request: ACK sip:test@5.135.179.50:6000
404	6.331107	192.168.10.4	5.135.179.50	SIP	412	Request: BYE sip:test@5.135.179.50:6000
410	6.416112	5.135.179.50	192.168.10.4	SIP	403	Status: 200 OK (BYE)

```

Frame 4: 412 bytes on wire (3296 bits), 412 bytes captured (3296 bits)
Ethernet II, Src: Tp-LinkKT_06:df:2c (64:66:b3:06:df:2c), Dst: Sagemcom_9d:a3:ed (88:a6:c6:9d:a3:ed)
Internet Protocol Version 4, Src: 192.168.10.4, Dst: 5.135.179.50
User Datagram Protocol, Src Port: 5090, Dst Port: 6000
Session Initiation Protocol (ACK)

0000  88 a6 c6 9d a3 ed 64 66 b3 06 df 2c 08 00 45 00  ....df...,..E
0001  01 8e 73 17 00 00 80 11 00 00 c0 a8 0a 04 85 87  ..s.....
0002  b3 32 13 e2 17 78 01 7a 84 f1 41 43 4b 29 73 69  2...p.z..ACK si
0003  78 3a 74 65 73 74 40 35 2e 31 33 35 2e 31 37 39  p;test@5.135.179
0004  2e 35 30 3a 36 38 30 30 28 53 49 56 2f 32 2e 30  .50:6000 SIP/2.0.
0005  0d 0a 56 69 61 3a 20 53 49 56 2f 32 2e 30 2f 55  ..Via: S IP/2.0/U
0006  44 50 20 31 39 32 2e 31 36 38 2e 31 39 2e 34 3a  DP 192.168.10.4
0007  35 30 39 38 3b 72 70 6f 72 74 3b 62 72 61 6e 63  5090;rpo rt;branc
0008  68 3d 7a 39 68 47 34 62 4b 56 6a 36 39 36 66 62  h=zsh645:KPJ666fb
0009  66 31 66 66 61 35 37 34 35 34 34 61 34 39 65 36  fffffa574 544a49e6

Session Initiation Protocol: Protocol
Packets: 412 - Displayed: 6 (1.6%)

```

406 VoIP calls are displayed as shown in the bottom right of the screen shot Packets: 412 Displayed: 406(98.5%)

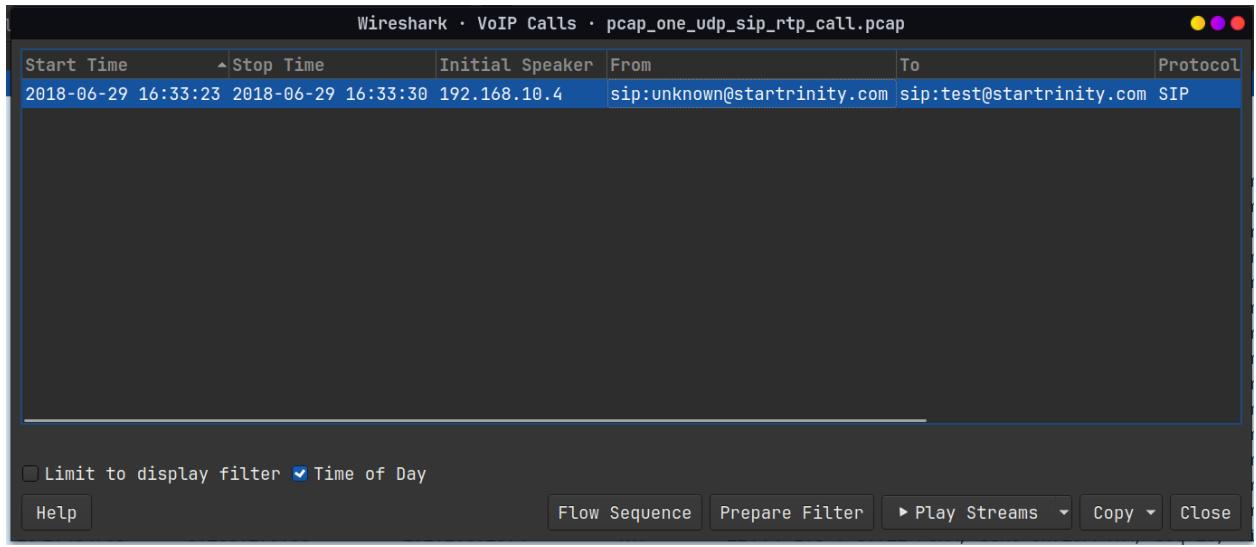
No.	Time	Source	Destination	Protocol	Length	Info
5 2 .298730	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=0, Time=1539072411
6 2 .319765	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=1, Time=1539072751
7 2 .338863	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=2, Time=1539072731
8 2 .358783	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=3, Time=1539072891
9 2 .378754	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=4, Time=1539073051
10 2 .389739	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=5, Time=1539073211
11 2 .408112	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=6, Time=1491300898
12 2 .418740	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=7, Time=1539073371
13 2 .427115	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=8, Time=1491301058
14 2 .437953	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=9, Time=1539073531
15 2 .439795	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=10, Time=1539073691
16 2 .458754	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=11, Time=1539073691
17 2 .468269	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=12, Time=1491301378
18 2 .478716	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=13, Time=1539073851
19 2 .484768	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=14, Time=1491301538
20 2 .498761	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=15, Time=1539074011
21 2 .509284	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=16, Time=1491301598
22 2 .515156	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=17, Time=1539074158
23 2 .538752	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=18, Time=1491301717
24 2 .538753	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=19, Time=1539074331
25 2 .547437	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=20, Time=1491302030
26 2 .558758	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=21, Time=1539074491
27 2 .562612	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=22, Time=1491302178
28 2 .577619	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=23, Time=1491302338
29 2 .578748	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=24, Time=1539074651
30 2 .598745	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=25, Time=1539074811
31 2 .669278	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=26, Time=1491302498
32 2 .618631	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=27, Time=1539074971
33 2 .624247	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=28, Time=1491302658
34 2 .638631	192.168.10.4	5.135.179.50	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=29, Time=1539075131
35 2 .640788	5.135.179.50	192.168.10.4	RTP	214	Pt=ITU-T G.711 PCMA	SSRC=0xC8280778, Seq=30, Time=1491302818

Frame 5: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
 Ethernet II, Src: Tp-LinkT_06:df:2c (64:66:b3:06:df:2c), Dst: Sagemcom_9d:a3:ed (08:a6:c6:9d:a3:ed)
 Internet Protocol Version 4, Src: 192.168.10.4, Dst: 5.135.179.50
 User Datagram Protocol, Src Port: 21500, Dst Port: 26000
 Real-Time Transport Protocol

..... df , E
 0000 00 c8 11 11 00 00 00 11 a4 f0 c0 a8 04 05 b7 2S e [
 0001 61 9b c8 28 d5 9b 00 00 00 00 00 00 00 00 00 00 a (x
 0002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
 0003 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
 0004 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
 0005 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
 0006 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
 0007 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
 0008 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
 0009 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..
 Activate WiFi
 Go-to Settings

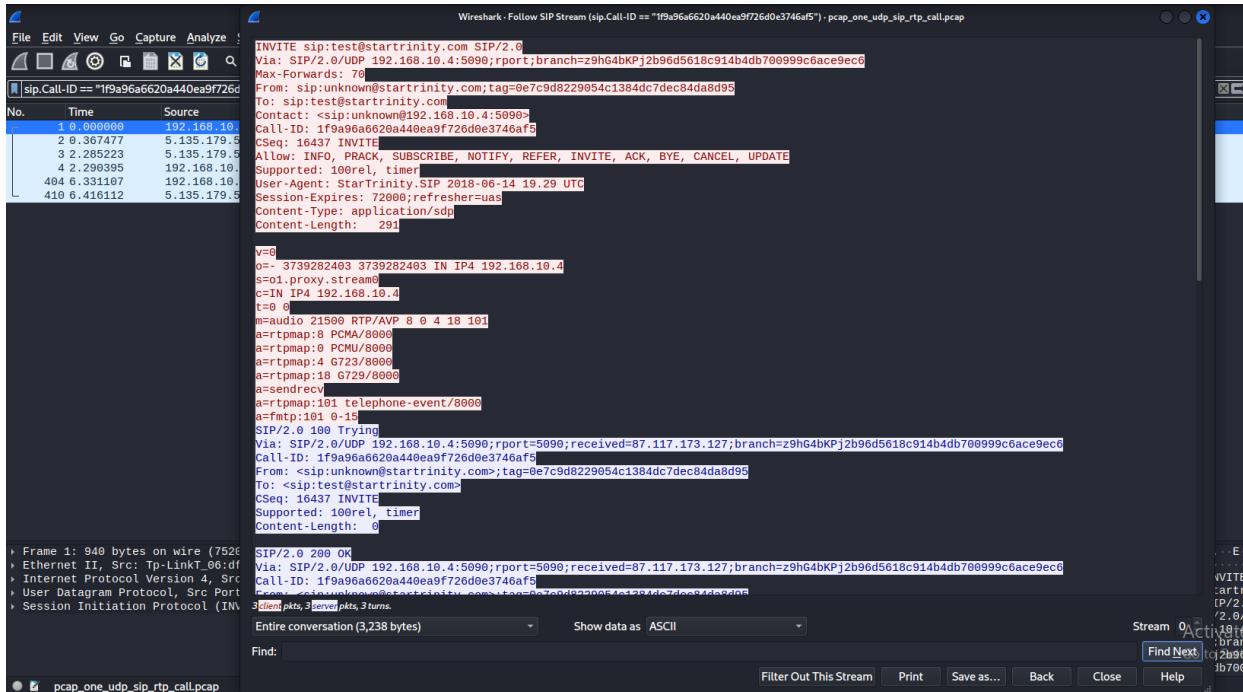
Packets: 412 - Displayed: 406 (98.5%)

Task2.3:



Task2.4:

Time	192.168.10.4	5.135.179.50	Comment
0.000000	5090 INVITE SDP (g711A g711U g723 g729 telephone..	6000	SIP INVITE From: sip:unknown@startrinity.com ..
0.367477	5090 < 100 Trying	6000	SIP Status 100 Trying
2.285223	5090 < 200 OK SDP (g711A g711U g723 g729 telephone..	6000	SIP Status 200 OK
2.290395	5090 < ACK	6000	SIP Request INVITE ACK 200 CSeq:16437
2.298730	21500 RTP (g711A)	26000	RTP, 203 packets. Duration: 4.04s SSRC: 0xC82..
2.408112	21500 < RTP (g711A)	26000	RTP, 203 packets. Duration: 4.03s SSRC: 0x710..
6.331107	5090 < BYE	6000	SIP Request BYE CSeq:16438
6.416112	5090 < 200 OK	6000	SIP Status 200 OK



Wireshark - Follow SIP Stream (sip.Call-ID == "1f9a96a6620a440ea9f726d0e3746af5") - pcap_one_udp_sip_rtp_call.pcap

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.10.4:5090; rport=5090;received=87.117.173.127;branch=z9hG4bKPj2b96d5618c914b4db700999c6ace9ec6
Call-ID: 1f9a96a6620a440ea9f726d0e3746af5
From: <sip:unknown@startrinity.com>;tag=0e7c9d8229054c1384dc7dec84da8d95
To: <sip:test@startrinity.com>;tag=7d669b078fe64689b403338d6d73ee46
CSeq: 16437 INVITE
Supported: 100rel, timer
Content-Type: application/sdp
Content-Length: 291

v=0
o= 3739271587 3739271587 IN IP4 5.135.179.50
s=1.proxy.stream0
c=IN IP4 5.135.179.50
t=0
m=audio 26000 RTP/AVP 8 0 4 18 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:4 G723/8000
a=rtpmap:18 G729/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
ACK sip:test@5.135.179.50:6000 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.4:5090; rport;branch=z9hG4bKPj600fb1ffa574544a49e63fd29a68101
Max-Forwards: 76
From: sip:unknown@startrinity.com;tag=0e7c9d8229054c1384dc7dec84da8d95
To: sip:test@startrinity.com;tag=7d669b078fe64689b403338d6d73ee46
Call-ID: 1f9a96a6620a440ea9f726d0e3746af5
CSeq: 16437 ACK
Content-Length: 0

BYE sip:test@5.135.179.50:6000 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.4:5090; rport;branch=z9hG4bKPj487d69b4835c46059705d65707e00950
Max-Forwards: 76
From: sip:unknown@startrinity.com;tag=0e7c9d8229054c1384dc7dec84da8d95
To: sip:test@startrinity.com;tag=7d669b078fe64689b403338d6d73ee46
Call-ID: 1f9a96a6620a440ea9f726d0e3746af5
CSeq: 16437 BYE
Content-Length: 0

Frame 1: 940 bytes on wire (7520 bits), 940 bytes captured (7520 bits)
Ethernet II, Src: TP-Link_06:d1 (08:00:00:06:d1:01), Dst: StarTrinity_00:0c:00 (08:00:00:00:0c:00)
Internet Protocol Version 4, Src: 192.168.10.4, Dst: 5.135.179.50
User Datagram Protocol, Src Port: 5090, Dst Port: 5090
Session Initiation Protocol (INVITE)

Stream 0 Active Find Next Find Previous
Client pkts, 3 server pkts, 3 turns.

Entire conversation (3,238 bytes) Show data as ASCII
Find: Filter Out This Stream Print Save as... Back Close Help

```

Frame 410: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits)
Ethernet II, Src: Sagemcom_9da3 (08:00:00:09:da:03), Dst: StarTrinity_00:0c:00 (08:00:00:00:0c:00)
Internet Protocol Version 4, Src: 192.168.10.4, Dst: 5.135.179.50
User Datagram Protocol, Src Port: 5090, Dst Port: 5090
Session Initiation Protocol (INVITE)

Stream 0 Active Find Next Find Previous
Client pkts, 3 server pkts, 3 turns.

Entire conversation (3,238 bytes) Show data as ASCII
Find: Filter Out This Stream Print Save as... Back Close Help

Scenario 3: Password Cracking using HashCat and John the ripper tools

Task3.1:

```

└─(tarek㉿kali)-[~]
└─$ curl -L "https://drive.google.com/uc?export=download&id=19YtGKWFACX6pibwtHMtx25JT_hEuUm6Q" -o complex_hash.txt
  % Total    % Received % Xferd  Average Speed   Time   Time     Time  Current
          Dload  Upload Total Spent   Left Speed
  0      0     0      0     0       0      0 --:--:-- --:--:-- --:--:-- 0
100  168  100  168     0       0    111      0  0:00:01  0:00:01 --:--:-- 84000

└─(tarek㉿kali)-[~]
└─$ cat complex_hash.txt
8a24367a1f46c141048752f2d5bbd14b
4ece57a61323b52ccffdbef021956754
78d8707579eab0695d5eaf80b072df14
b2d5d613de0611a5e71110c381dc63dc
7e62797fbcd4b3e787d1364cae3cf263

└─(tarek㉿kali)-[~]
└─$ 

```

Activate Windows
Go to Settings to activate


```

└─(tarek㉿kali)-[~]
└─$ curl -L "https://drive.google.com/uc?export=download&id=1BaGW_9c1_KWRzRehcvW_LJj0lYJtV66c" -o simple_hash.txt
  % Total    % Received % Xferd  Average Speed   Time   Time     Time  Current
          Dload  Upload Total Spent   Left Speed
  0      0     0      0     0       0      0 --:--:-- --:--:-- --:--:-- 0
100  170  100  170     0       0    116      0  0:00:01  0:00:01 --:--:-- 432

└─(tarek㉿kali)-[~]
└─$ cat simple_hash.txt
203ad5ffa1d7c650ad681fdff3965cd2
bd1d7b0809e4b4ee9ca307aa5308ea6f
e99a18c428cb38d5f260853678922e03
8afa847f50a716e64932d995c8e7435a
3b03c7ea09871a75dce2e403ef28111f

└─(tarek㉿kali)-[~]
└─$ 

```

Activate Windows
Go to Settings to activate

The used algorithm is MD5.

```

└─(tarek㉿kali)-[~]
└─$ hashid < complex_hash.txt
[...]
└─(tarek㉿kali)-[~]
└─$ hashid < simple_hash.txt
[...]

```

Task3.2:

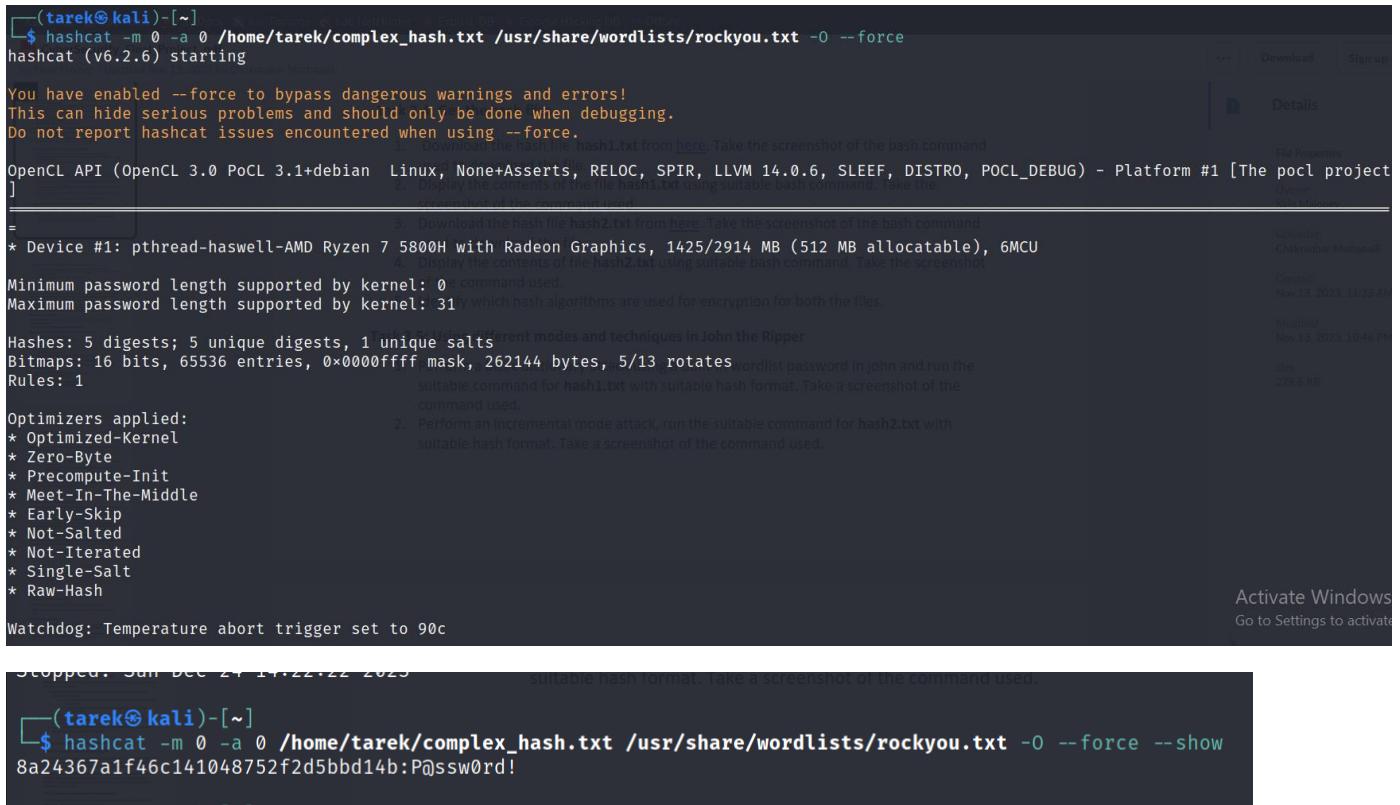
Its path: /usr/share/wordlists/rockyou.txt.gz

```
[~] (root㉿kali)-[~]
└─# find / -name rockyou.*  
find: '/run/user/1000/doc': Permission denied  
find: '/run/user/1000/gvfs': Permission denied  
/usr/share/wordlists/rockyou.txt.gz
```

Simple_hash.txt:

```
[~] (tarek㉿kali)-[~]
└─$ hashcat -m 0 -a 0 /home/tarek/simple_hash.txt /usr/share/wordlists/rockyou.txt -o --force  
hashcat (v6.2.6) starting ...  
  
You have enabled --force to bypass dangerous warnings and errors!  
This can hide serious problems and should only be done when debugging hashcat's built-in rules.  
Do not report hashcat issues encountered when using --force.  
1. Locate the built-in rockyou.txt wordlist file using a suitable command. Take a screenshot of the command used.  
2. Decrypt the hashes in the files simple_hash.txt and Complex_hash.txt using suitable hashcat commands. Take screenshots of the commands used.  
  
* Device #1: pthread-haswell-AMD Ryzen 7 5800H with Radeon Graphics, 1425/2914 MB (512 MB allocatable), 6MCU  
1. Document the cracked passwords and their corresponding plaintext results.  
Minimum password length supported by kernel: 0 strength and weaknesses of the cracked passwords based on the complexity  
Maximum password length supported by kernel: 31ash files.  
3. Take a screenshot of the outputs of the decryption.  
INFO: All hashes found as potfile and/or empty entries! Use --show to display them.  
  
Started: Sun Dec 24 13:37:22 2023 Task 3.4: Get the hash files  
Stopped: Sun Dec 24 13:37:22 2023 1. Download the hash file hash1.txt from here. Take the screenshot of the bash command used to download the file.  
2. Display the contents of the file hash1.txt using suitable bash command. Take the screenshot of the bash command used to download the file.  
203ad5ffa1d7c650ad681fdf3965cd2:hello1 Download the hash file hash2.txt from here. Take the screenshot of the bash command used to download the file.  
bd1d7b0809e4b4ee9ca307aa5308ea6f:mon e99a18c428cb38df260853678922e03:abc123 Display the contents of file hash2.txt using suitable bash command. Take the screenshot of the command used.  
8afa847f50a716e64932d995c8e7435a:princess 3b03c7ea09871a75dce2e403ef28111f:happy1 Identify which hash algorithms are used for encryption for both the files.  
  
Activate Window  
Go to Settings to ac
```

Complex_hash.txt:



The screenshot shows a file sharing interface with a file named "Complex_hash.txt". The file content is a terminal session of the hashcat tool. The session details are as follows:

- Hashcat version: v6.2.6
- Platform: OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 14.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
- Device: #1: pthread-haswell-AMD Ryzen 7 5800H with Radeon Graphics, 1425/2914 MB (512 MB allocatable), 6MCU
- Minimum password length supported by kernel: 0
- Maximum password length supported by kernel: 31
- Hashes: 5 digests; 5 unique digests, 1 unique salts
- Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
- Rules: 1
- Optimizers applied:
 - * Optimized-Kernel
 - * Zero-Byte
 - * Precompute-Init
 - * Meet-In-The-Middle
 - * Early-Skip
 - * Not-Salted
 - * Not-Iterated
 - * Single-Salt
 - * Raw-Hash
- Watchdog: Temperature abort trigger set to 90c

The command used was \$ hashcat -m 0 -a 0 /home/tarek/complex_hash.txt /usr/share/wordlists/rockyou.txt -o --force. A note says "Download the hash file hash1.txt from [here](#). Take the screenshot of the bash command".

Below the terminal session, there is a note: "Stopped. Sun Dec 24 14:22:22 2023" and "suitable hash format. Take a screenshot of the command used."

one hash was just found

Task3.3:

Simple_hash.txt

203ad5ffa1d7c650ad681fdff3965cd2:hello1

bd1d7b0809e4b4ee9ca307aa5308ea6f:mom

e99a18c428cb38d5f260853678922e03:abc123

8afa847f50a716e64932d995c8e7435a:princess

3b03c7ea09871a75dce2e403ef28111f:happy1

Complex_hash.txt

8a24367a1f46c141048752f2d5bbd14b:P@ssw0rd!

The simple_hash.txt was easy to crack as we used -a 0 which corresponds to straight but in complex_hash.txt just one hash was cracked and the other hashes was not crackable and was not fast as simple hash

Attack mode

```
0 = Straight  
1 = Combination  
3 = Brute-force  
6 = Hybrid Wordlist + Mask  
7 = Hybrid Mask + Wordlist
```

Output of simple_hash.txt:

```
(tarek㉿kali)-[~] 2. Decrypt the hashes in the files simple_hash.txt and Complex_hash.txt using suitable  
$ hashcat -m 0 -a 0 /home/tarek/simple_hash.txt /usr/share/wordlists/rockyou.txt -o --force --show  
hashcat commands. Take screenshots of the commands used.  
203ad5ffa1d7c650ad681fdff3965cd2:hello1  
bd1d7b0809e4b4ee9ca307aa5308ea6f:monk3.3 Analyzing cracked passwords and their implications.  
e99a18c428cb38d5f260853678922e03:abc123 Document the cracked passwords and their corresponding plaintext results.  
8afa847f50a716e64932d995c8e7435a:princess Analyze the strength and weaknesses of the cracked passwords based on the complexity  
3b03c7ea09871a75dce2e403ef28111f:happy1 of both the hash files.  
3. Take a screenshot of the outcomes of the decryption.
```

Output of complex_hash.txt:

```
Stopped. Sun Dec 24 14:22:22 2023 suitable hash format. Take a screenshot of the command used.  
(tarek㉿kali)-[~]  
$ hashcat -m 0 -a 0 /home/tarek/complex_hash.txt /usr/share/wordlists/rockyou.txt -o --force --show  
8a24367a1f46c141048752f2d5bbd14b:P@ssw0rd!
```

Task3.4:

```
(tarek㉿kali)-[~] $ curl -L "https://drive.google.com/uc?export=download&id=1uHHxXyPzwssUlWKLBRt0jpwHK1iyM1N3" -o hash1.txt
% Total    % Received % Xferd  Average Speed   Time: 0:00:01
Dload  Upload  Total   Spent  Left  Speed
0      0     0      0      0      0      0      0
100  168  100  168    0     0  116      0  0:00:01  0:00:01  --:--:-- 164k

```

Task 3.3 Analyzing cracked passwords and their implications.

1. Document the cracked passwords and their corresponding plaintext results.
2. Decrypt the hashes in the file `sample_hashes` and `hash1.txt` using suitable hash cracking command and tools.
3. Take a screenshot of the outcomes of the decryption.

Task 3.4: Get the hash files

1. Download the hash file `hash1.txt` from [here](#). Take the screenshot of the bash command used to download the file.
2. Display the contents of the file `hash1.txt` using suitable bash command. Take the

```
(tarek㉿kali)-[~] $ curl -L "https://drive.google.com/uc?export=download&id=1JLBAaUd3wcbzAs6JRnxNYitKFmLWRTqu" -o hash2.txt
% Total    % Received % Xferd  Average Speed   Time: 0:00:01
Dload  Upload  Total   Spent  Left  Speed
0      0     0      0      0      0      0      0
100  208  100  208    0     0  121      0  0:00:01  0:00:01  --:--:-- 121

```

(tarek㉿kali)-[~]

\$ cat hash2.txt

59c826fc854197cbd4d1083bce8fc00d0761e8b3
7288edd0fc3ffcbbe93a0cf06e3568e28521687bc
5a46b8253d07320a14cace9b4dcbf80f93dcef04
5049c40354ababd47f246f9204467548e39df6f8
23d42f5f3f66498b2c8ff4c20b8c5ac826e47146

The used algorithm in hash1 is MD5

```
(tarek㉿kali)-[~] $ hashid < hash1.txt
Analyzing '59c826fc854197cb'

```

The used algorithm in hash2 is SHA-1

```
(tarek㉿kali)-[~] $ hashid < hash2.txt
Analyzing '59c826fc854197cb'

```

Task3.5:

Hash1.txt:

```
[john@tarek-kali:~/Desktop]$ ./john hash1.txt --format=RAW-MD5
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=6
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
a1b2c3          (?)
flower          (?)
unix            (?)
Proceeding with incremental:ASCII
john123        (?)
rockstar       (?)
5g 0:00:01:06 DONE 3/3 (2023-12-24 14:34) 0.07560g/s 51439Kp/s 51439Kc/s 51461KC/s rockepon.. rockstay
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

Started Sat Dec 24 14:22:11 2023
[john@tarek-kali:~/Desktop]$ ./john hash1.txt --format=RAW-MD5 --show
?:a1b2c3
?:unix
?:flower F0c141048752F2d5bbd14b:Passw0rd!
?:john123
?:rockstar

5 password hashes cracked, 0 left
```

Hash2.txt:

```
[john@tarek-kali:~/Desktop]$ ./john hash2.txt --format=RAW-SHA1
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=6
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
```

```
(tarek㉿kali)-[~]
$ john hash2.txt --format=RAW-SHA1 --show
?:cookie
?:test123
?:flower

3 password hashes cracked, 2 left
```

Task3.6:

Hash1.txt

3c086f596b4aee58e1d71b3626fefc87:a1b2c3

4913a9178621eadcdf191db17915fbcb:unix

608f0b988db4a96066af7dd8870de96c:flower

6e0b7076126a29d5dfcbd54835387b7b:john123

d2feb9b6718bb374dfdd689380676954:rockstar

```
(tarek㉿kali)-[~] 22-11-2023
$ john hash1.txt --format=RAW-MD5 --show
?:a1b2c3@kali:[~]
?:unix:[~]cat -m 0 -a 0 /home/tarek/complex_hash.txt /usr/share/wordlists/rockyou.txt -o --force --show
?:flower f46c141048752f2d5bbd14b:P@ssw0rd!
?:john123
?:rockstar
[tarek㉿kali)-[~]

5 password hashes cracked, 0 left
```

Hash2.txt

59c826fc854197cbd4d1083bce8fc00d0761e8b3:cookie

7288edd0fc3fffbe93a0cf06e3568e28521687bc:test123

5a46b8253d07320a14cace9b4dc80f93dcef04:flower

5049c40354ababd47f246f9204467548e39df6f8: NOT FOUND

23d42f5f3f66498b2c8ff4c20b8c5ac826e47146: NOT FOUND

```
(tarek㉿kali)-[~]
└─$ john hash2.txt --format=RAW-SHA1 --show
?:cookie
?:test123
?:flower

3 password hashes cracked, 2 left
```

While analyzing the strengths and weaknesses of the cracked passwords I found that the passwords were easy to crack as they were popular words and sequences in John the Ripper, apart from the last two hashes where the tool couldn't crack it.

Scenario 4: Manual SQL injection

Task4.1:



MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features.

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/openapi>.

Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2023, HCL Technologies, Ltd., All rights reserved.

Activate Windows
Go to Settings to activate Windows.

Task4.2:

Transaction ID	Transaction Time	Account ID	Action	Amount
12834	2023-12-24 13:49	800001	Deposit	\$1000.00
12833	2023-12-24 13:49	800000	Withdrawal	-\$1000.00

Task4.3:

1. The website is at risk of SQL injection

a- The website is at risk of SQL injection, which can result in significant consequences. An unauthorized attacker could exploit input vulnerabilities to execute SQL commands, potentially exposing, altering, or even deleting data.

b- To reduce the risk of SQL injection, employing parameterized queries and prepared statements can be effective measures.

2. Username: tarek' or 1=1--

Password: anypasswordcanwork

SELECT * FROM users WHERE

Username: 'tarek' or 1=1--'

Password: 'any password can work'

-- character ignores the part after its position. So the query only checks the username and the attacker will gain access to the admin account.

Username:

Password:

3.

The screenshot shows a web application interface for 'Altoro Mutual'. At the top, there's a green banner with icons for 'Sign Off', 'Contact Us', 'Feedback', and a search bar. Below the banner, the 'DEMO SITE ONLY' logo is visible. The main content area has tabs for 'PERSONAL' and 'SMALL BUSINESS'. On the left, a sidebar titled 'MY ACCOUNT' lists options like 'View Account Summary', 'View Recent Transactions', 'Edit Profile', 'Search News Articles', and 'Customer Site Language'. Another sidebar titled 'ADMINISTRATION' includes 'Edit Users'. The central content area displays a message 'Hello Admin User' and 'Welcome to Altoro Mutual Online.' It shows an account detail 'View Account Details: 800000 Corporate' with a 'GO' button. A 'Congratulations!' message states: 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply.' At the bottom, there's a note about the website being a demo and a copyright notice: 'Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2023, HCL Technologies, Ltd. All rights reserved.'

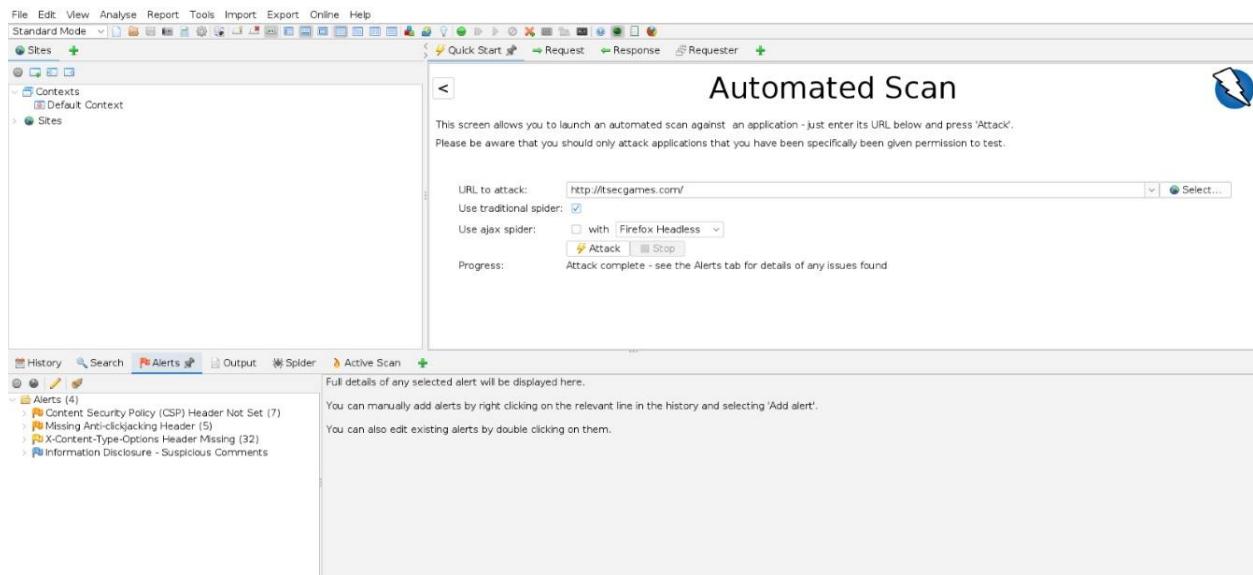
Scenario 5: Running pen-tests on a website using ZAP

Task5.1:

1. Conducting active scanning in the Zed Attack Proxy (ZAP) entails utilizing a conventional spider to navigate through a specified application. Following the setup of ZAP and the configuration of browser proxy settings, the spider is activated to survey the application's architecture. After the spidering process concludes, automated scanning is triggered, actively searching for vulnerabilities based on the identified structure. Subsequently, the

findings are assessed, with vulnerabilities being classified according to their severity. ZAP facilitates the creation of comprehensive reports, facilitating the examination and resolution of security concerns. It is imperative to execute such scans with proper authorization and adhere to ethical hacking principles to ensure responsible and lawful practices.

2.

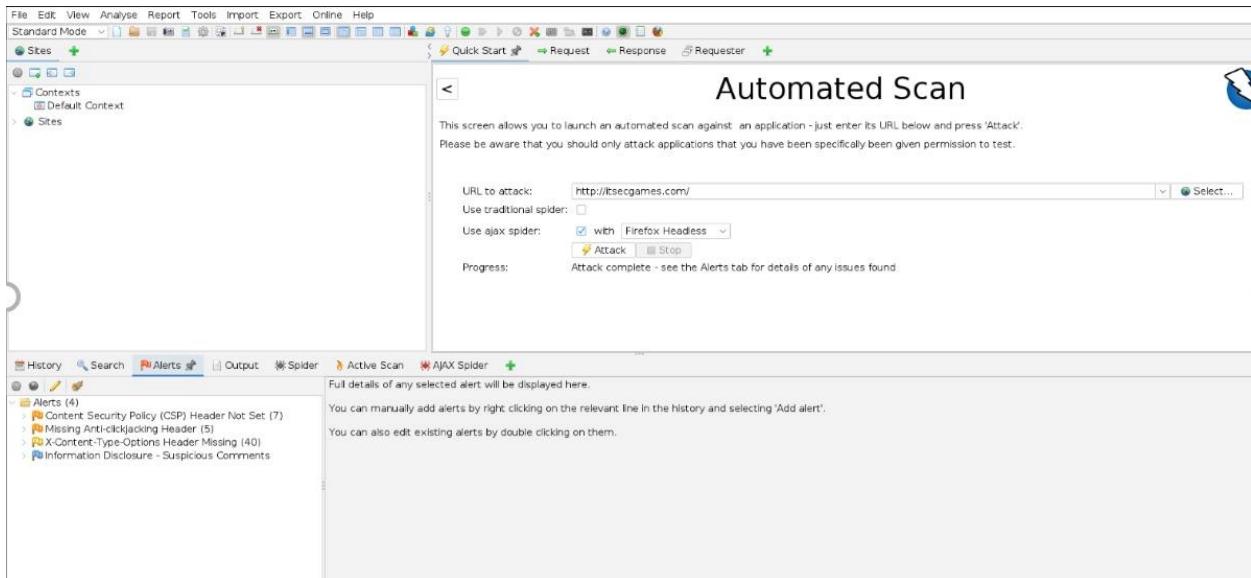


Task5.2:

1. To automate scanning using the Ajax Spider feature in Zed Attack Proxy (ZAP), start by configuring ZAP and setting up the browser to use ZAP as a proxy. In the Ajax Spider section, define the target URL and initiate the dynamic crawling process, allowing the tool to handle asynchronous requests and discover dynamic content, including interactions driven by JavaScript. After the spidering completes, transition to the Automated Scan tab, configure scan settings, and begin the automated scanning process. ZAP actively sends requests, incorporating insights gained from the Ajax Spider, to identify and evaluate vulnerabilities within the target application. Examine the comprehensive scan results and generate detailed reports through ZAP. It's crucial to conduct these scans with proper authorization and adhere to ethical

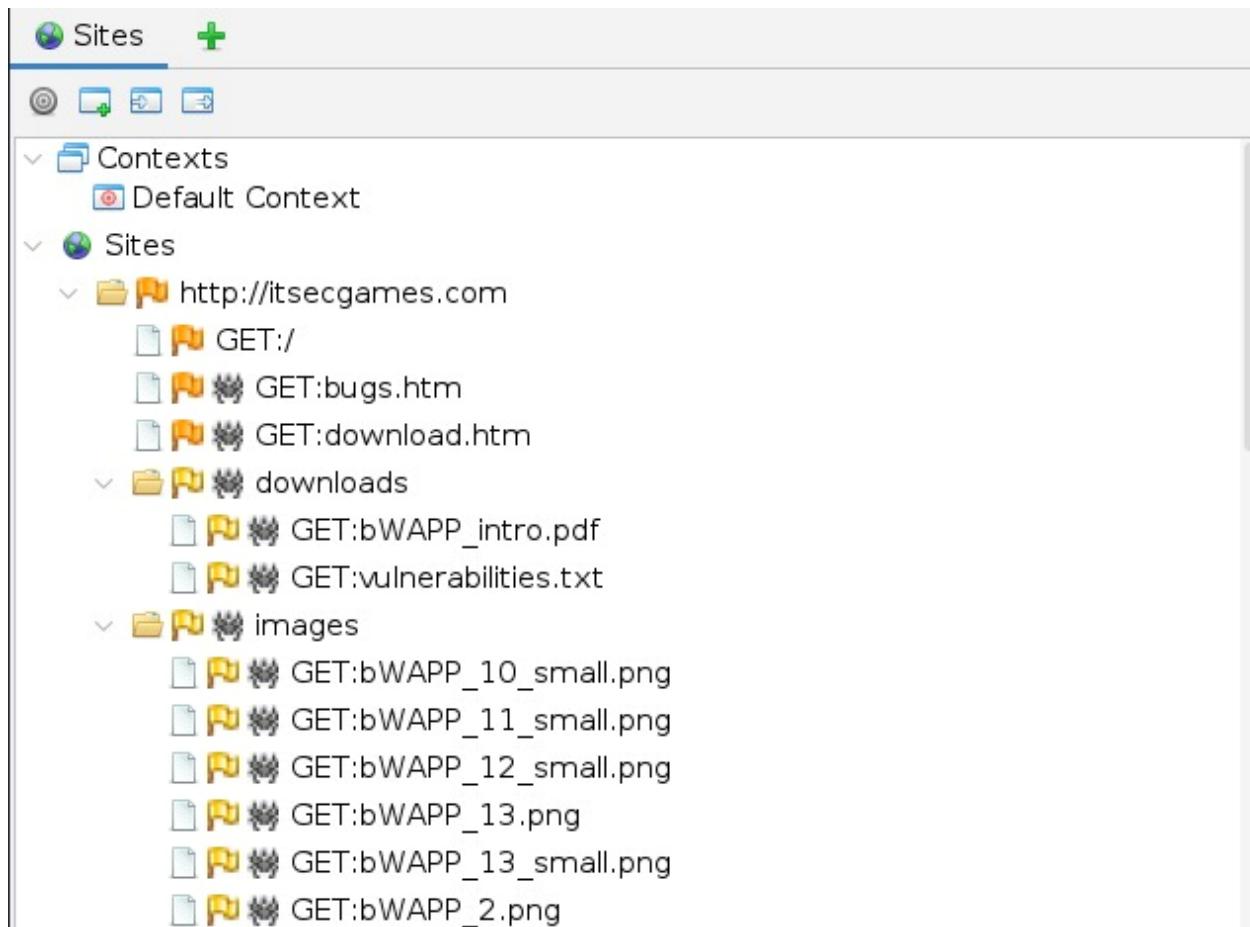
hacking principles for responsible and lawful security testing.

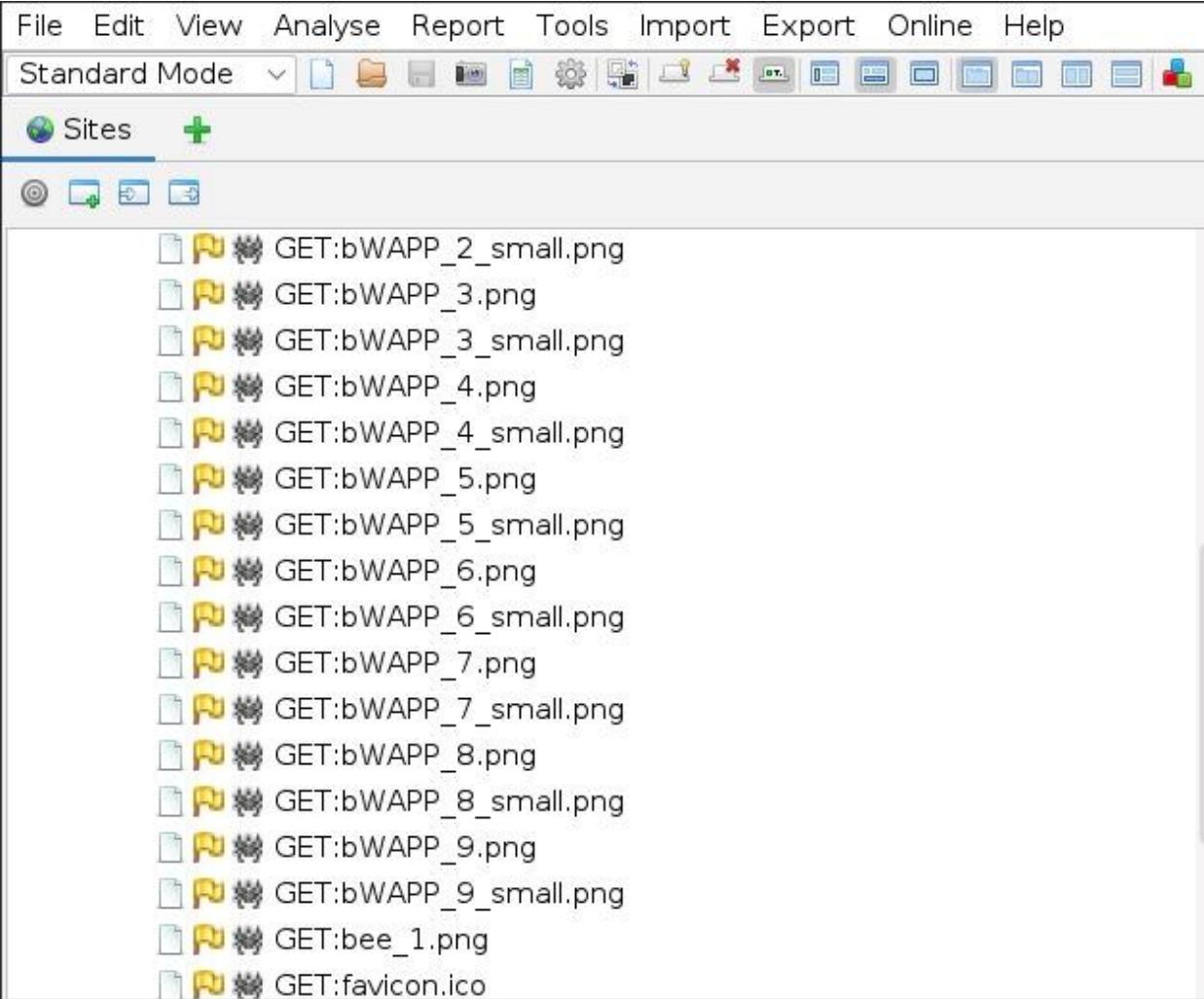
2.

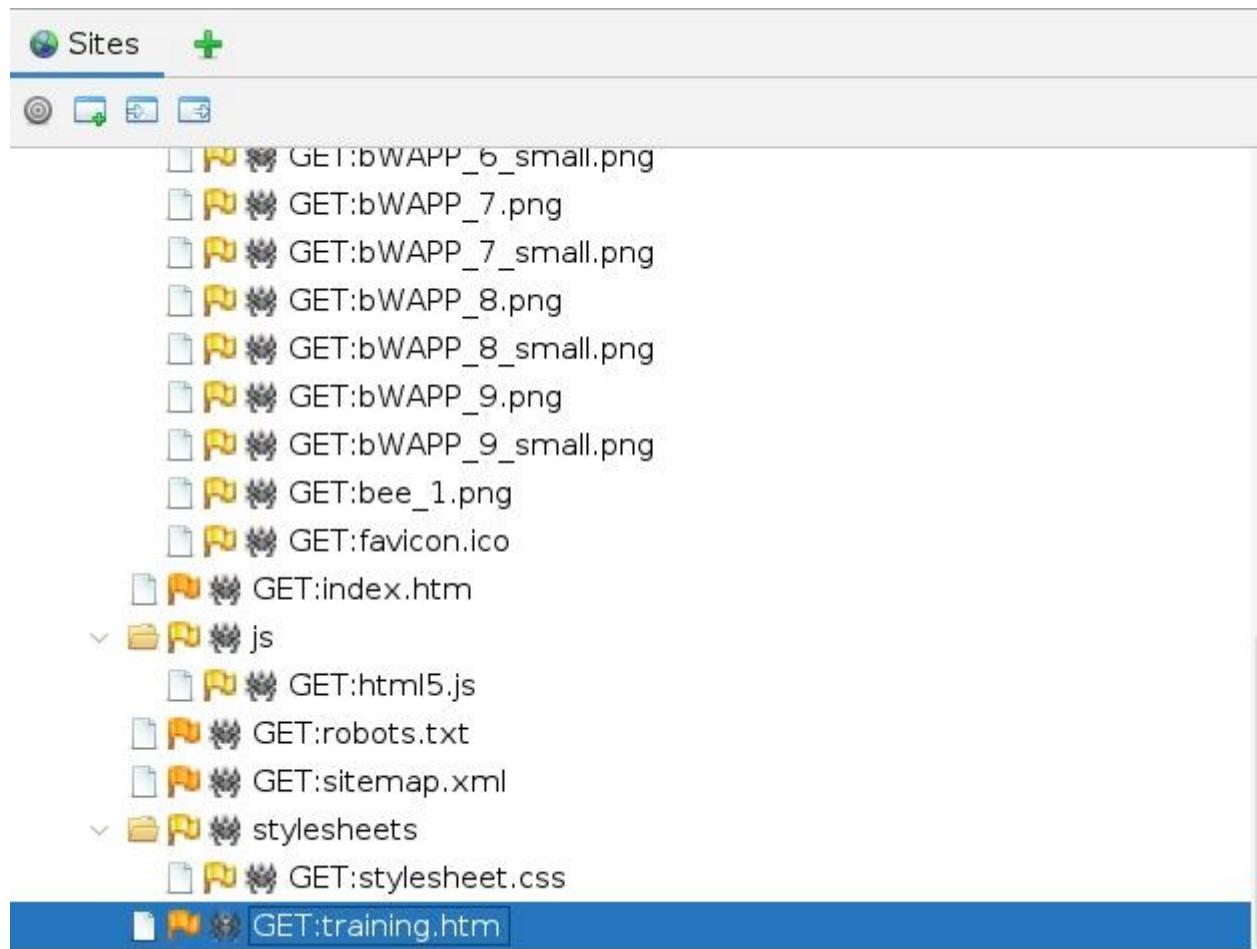


Task5.3:

1.Traditional spider tree







2.ajax spider tree



