SHARKFEST'14

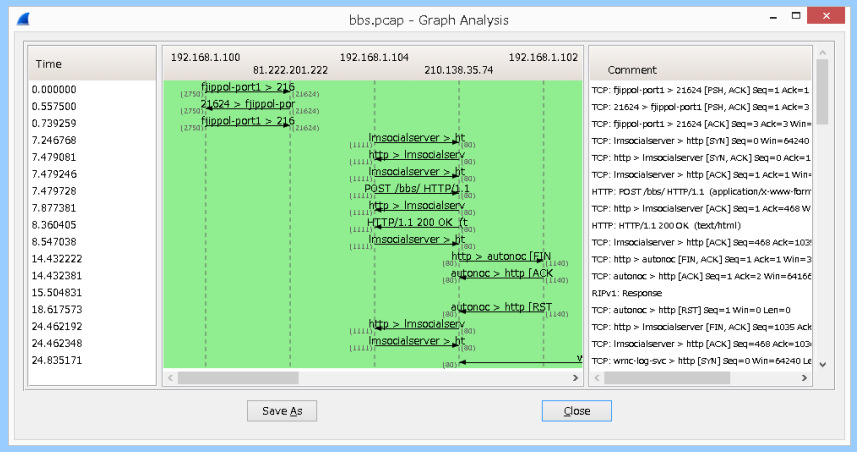
WIRESHARK DEVELOPER AND USER CONFERENCE

JUNE 16-20 2014 · DOMINICAN UNIVERSITY

Handsome Flow Graph

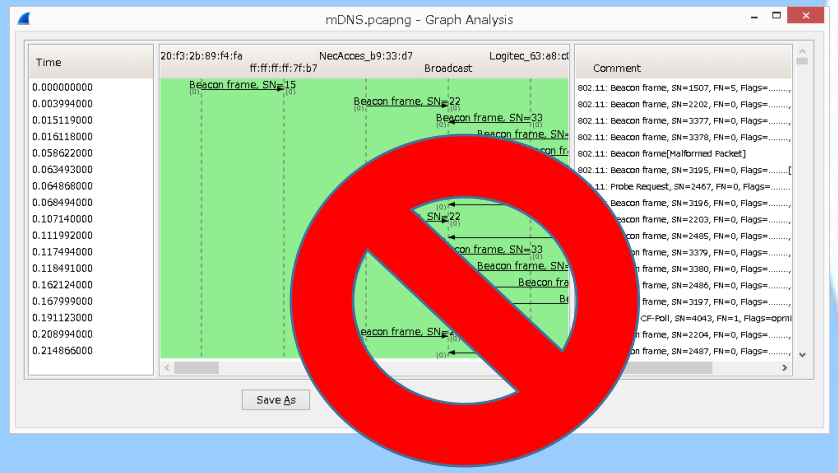
Megumi Takeshita,
Packet otaku
ikeriri network service co.,ltd

Flow Graph is convenient !



- Easy to Visualize
- Easy to understand
- Especially easy to encourage not-packet people to explain

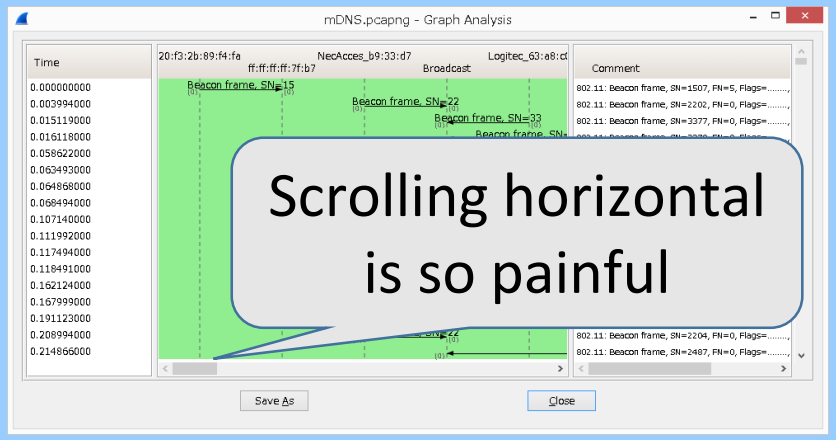
Flow Graph is inconvenient (´▪ω▪`)

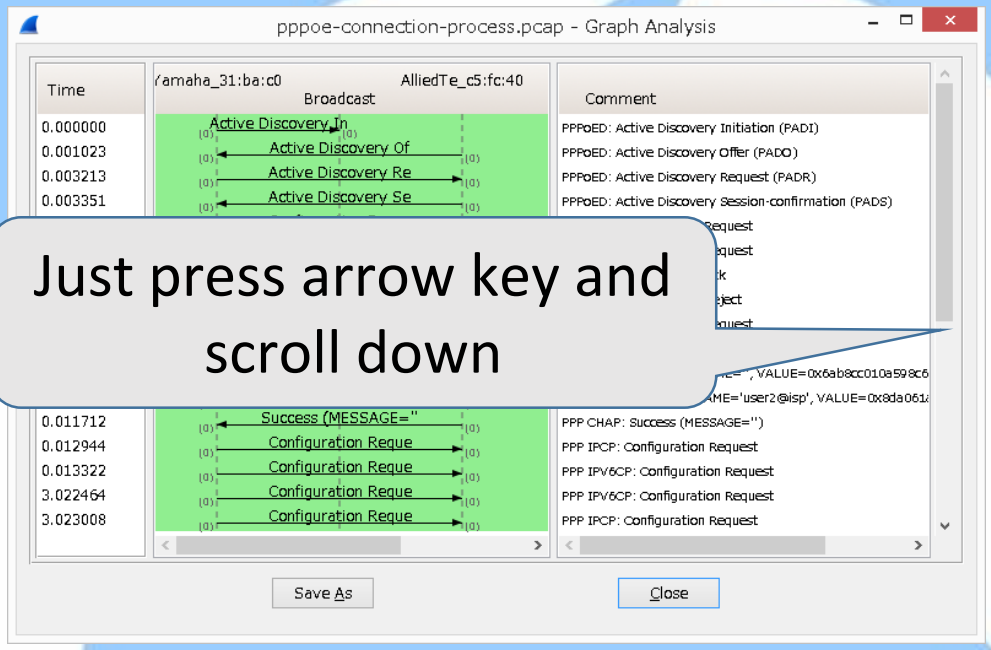


- Difficult to understand dulation (time lag)
- Difficult when traffic is large (especially 10 more nodes)
- Difficult when flow continues long and need to scroll a lot

Quick TIPS for Good Looking

- Filter traffic less than screen width





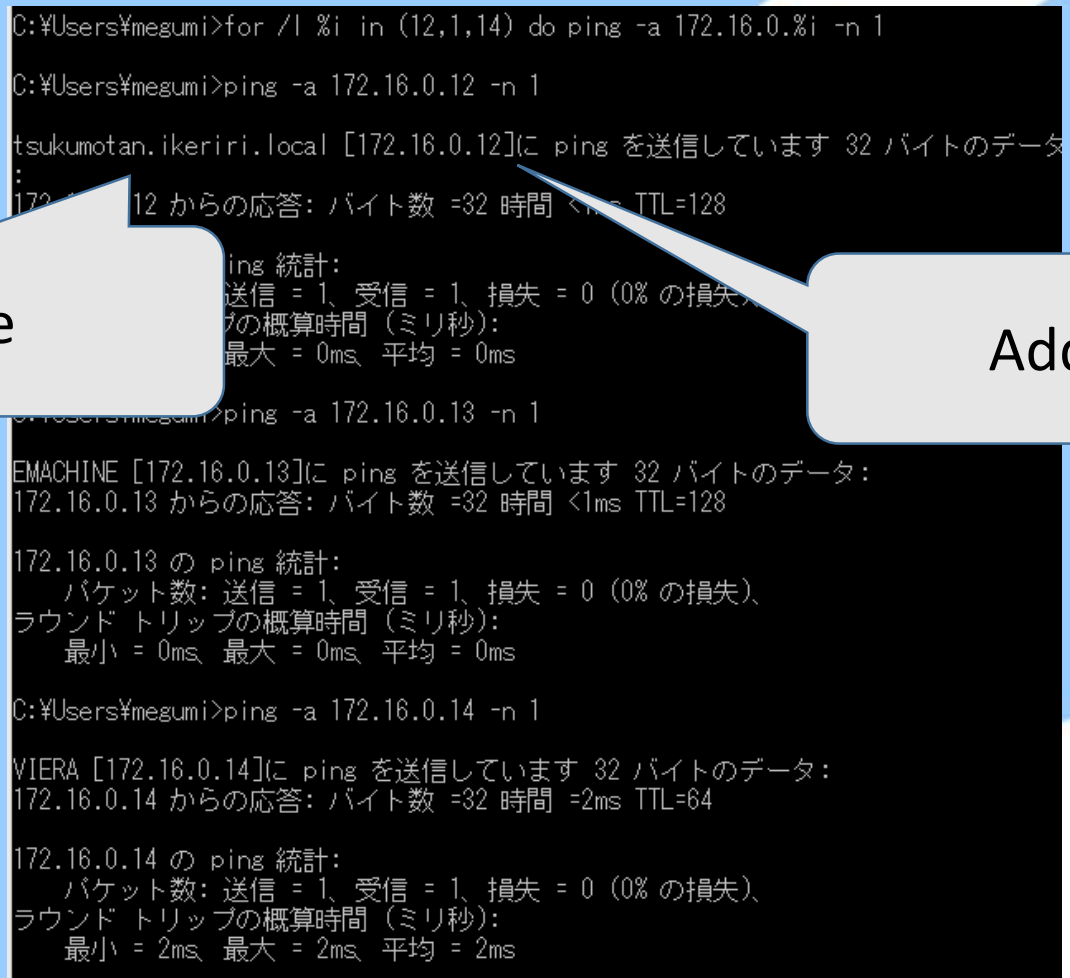
- Use aliases for multilayer (eth / ip)

  manuf and hosts (don’t forget to enable name resolution and disable external name server)

Use ping –a and get IP with Name

- At First look for computer name and IP address

  for /l %i in (12,1,14) do ping -a 172.16.0.%i -n 1

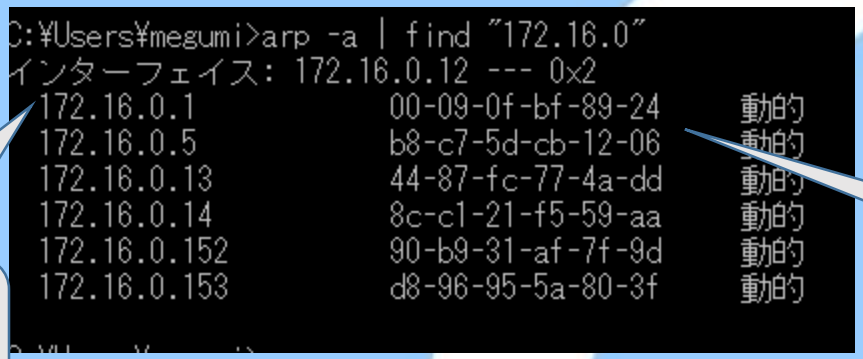


Name

Address

Use arp –a and get IP with MAC

- Then get IP address and MAC address
  arp -a | find "172.16.0"



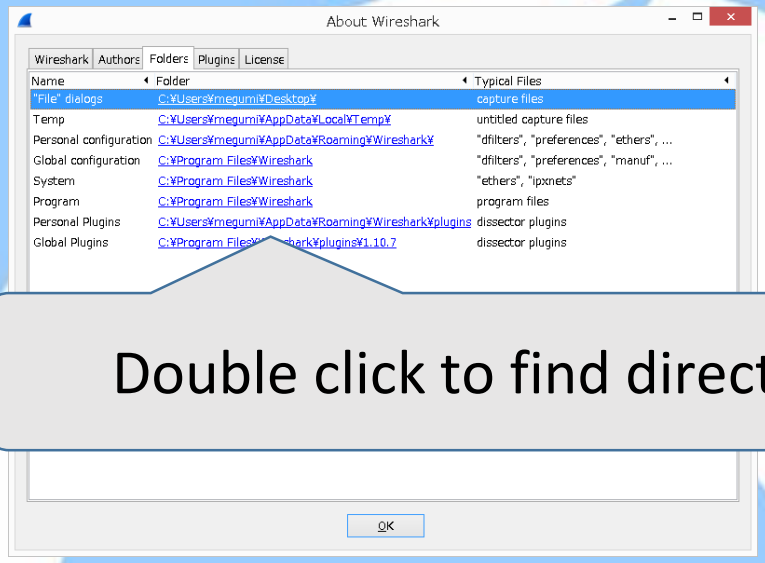
Address

MAC

Combine record and create files

- manuf (UTF-8/LN)
  add MAC IP

```
00:26:18:37:3A:50 tsukumotan_eth↓
44:87:fc:77:4a:dd emachine_eth↓
8c:c1:21:f5:59:aa viera_eth↓
↓
```



Double click to find directory

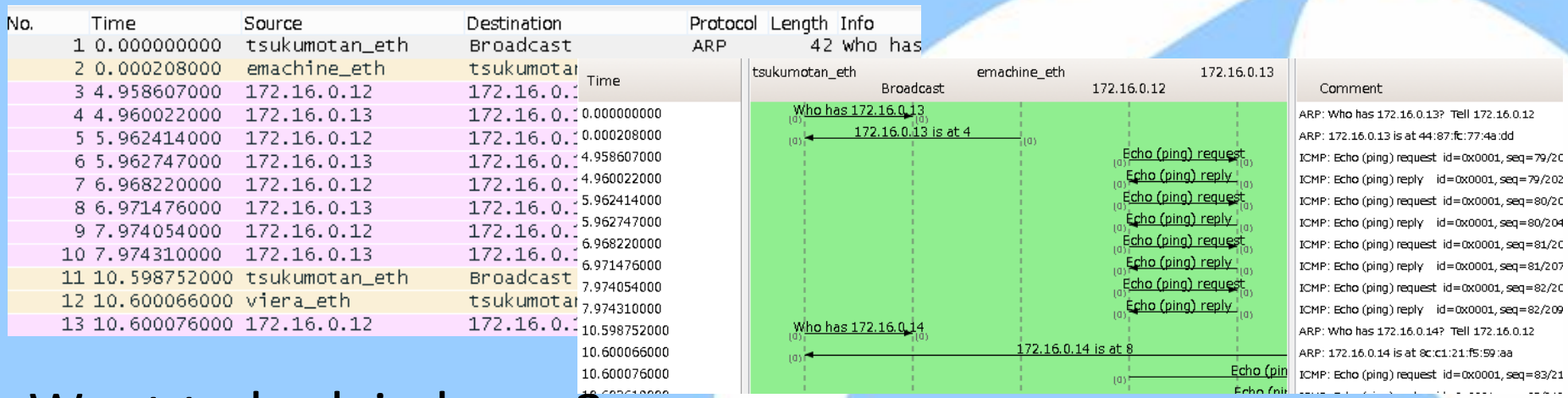
- Hosts (UTF-8/LN)
  add name IP

```
172.16.0.12 tsukumotanIP↓
172.16.0.13 emachine↓
172.16.0.14 viera [EOF]
```

Use same or related name
“tsukumotan_eth” in manuf
“tsukumotan” in hosts

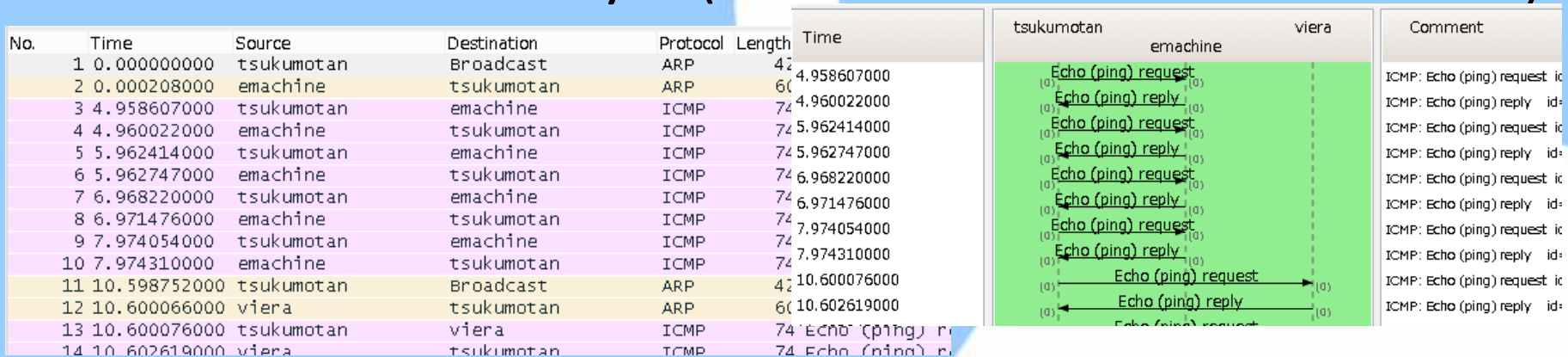
Somehow handsome ?

- Want to debug in layer 2
  (not use name resolution CheckOFF“enable network layer”)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	tsukumotan_eth	Broadcast	ARP	42	who has
2	0.000208000	emachine_eth	tsukumotan			
3	4.958607000	172.16.0.12	172.16.0.1			
4	4.960022000	172.16.0.13	172.16.0.1			
5	5.962414000	172.16.0.12	172.16.0.1			
6	5.962747000	172.16.0.13	172.16.0.1			
7	6.968220000	172.16.0.12	172.16.0.1			
8	6.971476000	172.16.0.13	172.16.0.1			
9	7.974054000	172.16.0.12	172.16.0.1			
10	7.974310000	172.16.0.13	172.16.0.1			
11	10.598752000	tsukumotan_eth	Broadcast			
12	10.600066000	viera_eth	tsukumotan			
13	10.600076000	172.16.0.12	172.16.0.1			

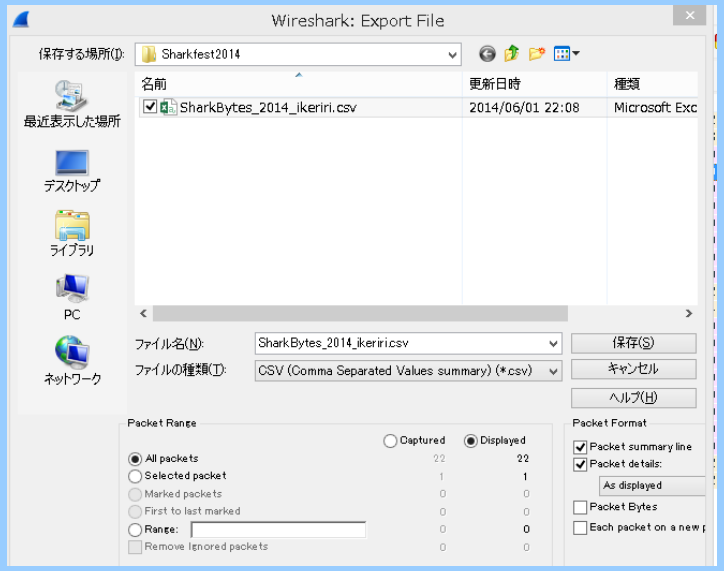
- Want to look in layer 3
  Enable for network layer (not use external name resolver)



No.	Time	Source	Destination	Protocol	Length
1	0.000000000	tsukumotan	Broadcast	ARP	42
2	0.000208000	emachine	tsukumotan	ARP	60
3	4.958607000	tsukumotan	emachine	ICMP	74
4	4.960022000	emachine	tsukumotan	ICMP	74
5	5.962414000	tsukumotan	emachine	ICMP	74
6	5.962747000	emachine	tsukumotan	ICMP	74
7	6.968220000	tsukumotan	emachine	ICMP	74
8	6.971476000	emachine	tsukumotan	ICMP	74
9	7.974054000	tsukumotan	emachine	ICMP	74
10	7.974310000	emachine	tsukumotan	ICMP	74
11	10.598752000	tsukumotan	Broadcast	ARP	42
12	10.600066000	viera	tsukumotan	ARP	60
13	10.600076000	tsukumotan	viera	ICMP	74
14	10.602619000	viera	tsukumotan	ICMP	74

More handsome looking ?

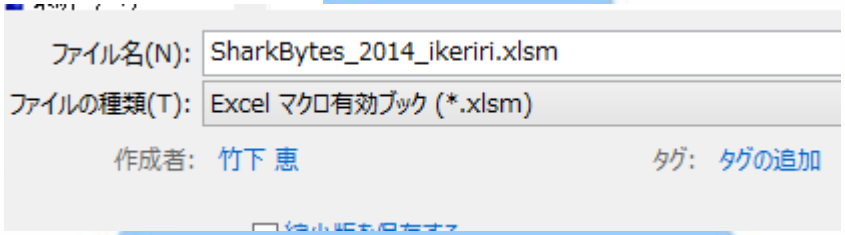
- First export CSV from Wireshark (Export packet dissectors as CSV)
- Use Excel or some tools to recognize duration from CSV files exported from Wireshark
- Creating macro to adjust row's width according to time duration (I hope wireshark do so)



	A	B	C	D	E	F	G
1	No.	Time	Source	Destination	Protocol	Length	Info
2	1	0	tsukumotar	Broadcast	ARP	42	Who has 172.16.0.13? Tell 172.16.0.12
3	2	0.000208	emachine	tsukumotar	ARP	60	172.16.0.13 is at 44:87:fc:77:4a:dd
4	3	4.958607	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=128 (reply in 4)
5	4	4.960022	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=79/20224, ttl=128 (request in 3)
6	5	5.962414	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=80/20480, ttl=128 (reply in 6)
7	6	5.962747	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=80/20480, ttl=128 (request in 5)
8	7	6.96822	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=81/20736, ttl=128 (reply in 8)
9	8	6.971476	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=81/20736, ttl=128 (request in 7)
10	9	7.974054	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=82/20992, ttl=128 (reply in 10)
11	10	7.97431	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=82/20992, ttl=128 (request in 9)
12	11	10.59875	tsukumotar	Broadcast	ARP	42	Who has 172.16.0.14? Tell 172.16.0.12
13	12	10.60007	viera	tsukumotar	ARP	60	172.16.0.14 is at 8c:c1:21:f5:59:aa
14	13	10.60008	tsukumotar	viera	ICMP	74	Echo (ping) request id=0x0001, seq=83/21248, ttl=128 (reply in 14)
15	14	10.60262	viera	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=83/21248, ttl=64 (request in 13)
16	15	11.60394	tsukumotar	viera	ICMP	74	Echo (ping) request id=0x0001, seq=84/21504, ttl=128 (reply in 16)
17	16	11.60625	viera	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=84/21504, ttl=64 (request in 15)
18	17	12.61181	tsukumotar	viera	ICMP	74	Echo (ping) request id=0x0001, seq=85/21760, ttl=128 (reply in 18)
19	18	12.61225	viera	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=85/21760, ttl=64 (request in 17)
20	19	13.61962	tsukumotar	viera	ICMP	74	Echo (ping) request id=0x0001, seq=86/22016, ttl=128 (reply in 20)
21	20	13.62142	viera	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=86/22016, ttl=64 (request in 19)
22	21	15.59983	Fortinet_bf	tsukumotar	ARP	60	Who has 172.16.0.1? Tell 172.16.0.1
23	22	15.59985	tsukumotar	Fortinet_bf	ARP	42	172.16.0.12 is at 00:26:18:37:3a:50
24							

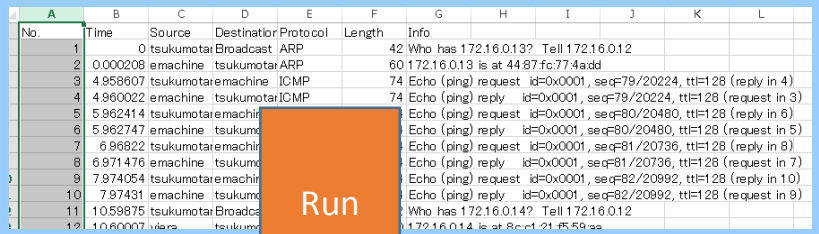
Create some macros

```
Sub set_duration()
    Dim i As Long
    Dim ln As Long
    Dim h As Long
    For i = 2 To 20
        'change Row Hight
        h = (Cells(i + 1, 1) - Cells(i, 1)) * 10
        Cells(i, 1).RowHeight = h
        'set RowHight
        ln = Cells(i, 1).RowHeight
     Next
End Sub
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0	tsukumotar	Broadcast	ARP	42	Who has 172.16.0.13? Tell 172.16.0.12
2	0.000208	emachine	tsukumotar	ARP	60	172.16.0.13 is at 44:87:fc:77:4a:dd
3	4.958607	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=128 (reply in 4)
4	4.960022	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=79/20224, ttl=128 (request in 3)
5	5.962414	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=80/20480, ttl=128 (reply in 6)
6	5.962747	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=80/20480, ttl=128 (request in 5)
7	6.96822	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=81/20736, ttl=128 (reply in 8)
8	6.971476	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=81/20736, ttl=128 (request in 7)
9	7.974054	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=82/20992, ttl=128 (reply in 10)
10	7.97431	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=82/20992, ttl=128 (request in 9)
11	10.59875	tsukumotar	Broadcast	ARP	42	Who has 172.16.0.14? Tell 172.16.0.12
12	10.60007	viera	tsukumotar	ARP	60	172.16.0.14 is at 8c:c1:21:f5:59:aa

Looking good ? Handsome !!



No.	Time	Source	Destination	Protocol	Length	Info
1	0	tsukumotar	Broadcast	ARP	42	Who has 172.16.0.13? Tell 172.16.0.12
2	0.000208	emachine	tsukumotar	ARP	60	172.16.0.13 is at 44:87:fc:77:4a:dd
3	4.958607	tsukumotar	emachine	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=128 (reply in 4)
4	4.960022	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=79/20224, ttl=128 (request in 3)
5	5.962414	tsukumotar	emachir			Echo (ping) request id=0x0001, seq=80/20480, ttl=128 (reply in 6)
6	5.962747	emachine	tsukumo			Echo (ping) reply id=0x0001, seq=80/20480, ttl=128 (request in 5)
7	6.96822	tsukumotar	emachir			Echo (ping) request id=0x0001, seq=81/20736, ttl=128 (reply in 8)
8	6.971476	emachine	tsukumo			Echo (ping) reply id=0x0001, seq=81/20736, ttl=128 (request in 7)
9	7.974054	tsukumotar	emachir			Echo (ping) request id=0x0001, seq=82/20992, ttl=128 (reply in 10)
10	7.97431	emachine	tsukumo			Echo (ping) reply id=0x0001, seq=82/20992, ttl=128 (request in 9)
11	10.59875	tsukumotar	Broadca			Who has 172.16.0.14? Tell 172.16.0.12
12	10.60007	viera	tsukumo			172.16.0.14 is at 8c:c1:21:ff:59:aa

Run macro

1	Time	Source	Destination	Protocol	Length	Info
3	0.000208	emachine	tsukumotar	ARP	60	172.16.0.13 is at 44:87:fc:77:4a:dd
5	4.960022	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=79/20224, ttl=128 (request in 3)
7	5.962747	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=80/20480, ttl=128 (request in 5)
9	6.971476	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=81/20736, ttl=128 (request in 7)
11	7.97431	emachine	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=82/20992, ttl=128 (request in 9)
15	10.60262	viera	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=83/21248, ttl=64 (request in 13)
17	11.60625	viera	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=84/21504, ttl=64 (request in 15)
19	12.61225	viera	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=85/21760, ttl=64 (request in 17)
21	13.62142	viera	tsukumotar	ICMP	74	Echo (ping) reply id=0x0001, seq=86/22016, ttl=64 (request in 19)
22	15.59983	Fortinet_bf:	tsukumotar	ARP	60	Who has 172.16.0.12? Tell 172.16.0.1
23	15.59985	tsukumotar	Fortinet_bf:	ARP	42	172.16.0.12 is at 00:26:18:37:3a:50
24						

TIME DURATION

Thank you