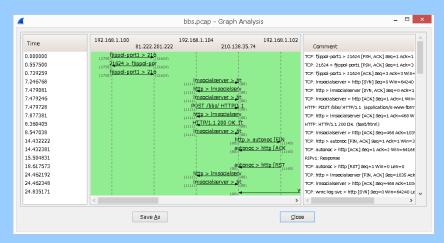


# Handsome Flow Graph

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

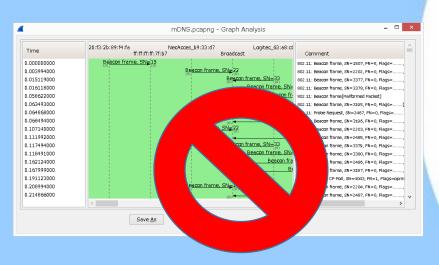


## Flow Graph is convenient!



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

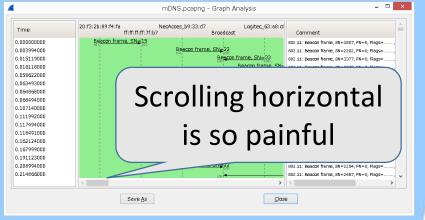
# Flow Graph is inconvenient ( •ω•`)

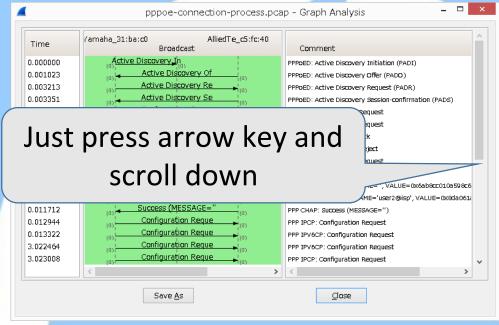


- Difficult to understand dulation (time lag)
- Difficult when traffic is large ( especially 10 more nodes)
- Difficult when flow continues long and need to scroll a lot

## 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

C:\Users\megumi>for /l %i in (12,1,14) do ping -a 172.16.0.%i -n 1

C:¥Users¥megumi>ping -a 172.16.0.12 -n 1

```
tsukumotan.ikeriri.local [172.16.0.12]に ping を送信しています 32 バイトのデータ
              送信 = 1、受信 = 1、損失 = 0(0% の損失
Name
                    'の概算時間(ミリ秒):
                                                             Address
                   最大 = Oms 平均 = Oms
                   ping -a 172.16.0.13 -n 1
        EMACHINE [172.16.0.13]に ping を送信しています 32 バイトのデータ:
        172.16.0.13 からの応答: バイト数 =32 時間 <1ms TTL=128
        172.16.0.13 の ping 統計:
          バケット数: 送信 = 1、受信 = 1、損失 = 0(0%の損失)、
        ラウンド トリッブの概算時間(ミリ秒):
           最小 = Oms、最大 = Oms、平均 = Oms
        C:\Users\megumi>ping -a 172.16.0.14 -n 1
        VIERA [172.16.0.14]に ping を送信しています 32 バイトのデータ:
        172.16.0.14 からの応答: バイト数 =32 時間 =2ms TTL=64
        172.16.0.14 の ping 統計:
```

バケット数: 送信 = 1、受信 = 1、損失 = 0(0%の損失)、

ラウンド トリップの概算時間 (ミリ秒): 最小 = 2ms、最大 = 2ms、平均 = 2ms

Sharkfest 2014

## Use arp —a and get IP with MAC

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

```
C:¥Users¥megumi>arp -a | find "172.16.0"
インターフェイス: 172.16.0.12 --- 0×2
172.16.0.1 00-09-0f-bf-89-24 動的
172.16.0.5 b8-c7-5d-cb-12-06 動的
172.16.0.13 44-87-fc-77-4a-dd 動的
172.16.0.14 8c-c1-21-f5-59-aa 動的
172.16.0.152 90-b9-31-af-7f-9d 動的
172.16.0.153 d8-96-95-5a-80-3f 動的
```

MAC

Address

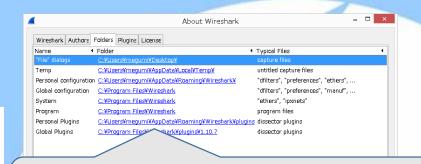
#### Combine record and create files

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↓
```

Hosts (UTF-8/LN)
 add name IP

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



Double click to find directory

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")

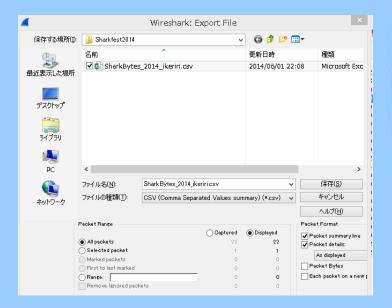
No.	Time	Source	Destination	Proto	col Length Info			
	1 0.000000000	tsukumotan_eth	Broadcast	ARP	42 Who has			
	2 0.000208000	emachine_eth	tsukumotar		tsukumotan_eth	emachine_eth	172.16.0.13	
	3 4.958607000	172.16.0.12	172.16.0.: Time		Broadcast		172.16.0.12	Comment
	4 4.960022000	172.16.0.13	172.16.0.10.000000000		Who has 172.16.0.13			ARP: Who has 172.16.0.13? Tell 172.16.0.12
	5 5.962414000	172.16.0.12	172.16.0.10.000208000		(0) 172.16.0.13 is at	4(0)		ARP: 172.16.0.13 is at 44:87:fc:77:4a:dd
	6 5.962747000	172.16.0.13	172.16.0.1 <sup>4.958607000</sup>		1		Echo (ping) request	ICMP: Echo (ping) request id=0x0001, seq=79/20
	7 6.968220000	172.16.0.12	172.16.0.: 4.960022000				Echo (ping) reply	ICMP: Echo (ping) reply id=0x0001, seq=79/202
	8 6.971476000	172.16.0.13	172 16 0 -5.962414000				Echo (ping) request	ICMP: Bcho (ping) request id=0x0001, seq=80/20
	9 7.974054000	172.16.0.12	172.16.0.15.962/4/000				Echo (ping) reply	ICMP: Echo (ping) reply id=0x0001, seq=80/204
	10 7.974310000	172.16.0.13	172.16.0. 6.971476000				Echo (ping) request	ICMP: Echo (ping) request id=0x0001, seq=81/20
	11 10.598752000	) tsukumotan_eth	Broadcast 7.974054000				Echo (ping) reply (a) Echo (ping) request	ICMP: Echo (ping) reply id=0x0001, seq=81/207
	12 10.600066000	_	tsukumotai 7.974310000		1 1	1	Echo (ping) reply	ICMP: Echo (ping) request id=0x0001, seq=82/20
	13 10.600076000	_	172.16.0.1 10.598752000		Who has 172.16.0_14		(a) Callo (ping) (epiv.)	ICMP: Echo (ping) reply id=0x0001, seq=82/209
			10.600066000		(d) (d)	172.16.0.	14 is at 8	ARP: Who has 172.16.0.14? Tell 172.16.0.12  ARP: 172.16.0.14 is at 8c:c1:21:f5:59:aa
			10.600076000		(0)	772.15.0.	Echo (pin	
			10.000070000			1	Echo (nit	zorn : bene (ping) request is altocoss, sed os, ss

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

								A	
		_			oath Time	tsukumotan	viera	Comment	
No.	Time	Source	Destination	Protocol Lei	ngth Time	emachine			
	1 0.000000000	tsukumotan	Broadcast	ARP	4.958607000	Echo (ping) request	1	ICMP: Echo (ping) request id	
	2 0.000208000	emachine	tsukumotan	ARP	6(	(0) (0)	100	" -7 '	
	3 4.958607000	tsukumotan	emachine	ICMP	74.960022000	Echo (ping) reply		ICMP: Echo (ping) reply id:	
	4 4.960022000	emachine	tsukumotan	ICMP	74 5.962414000	Echo (ping) request		ICMP: Echo (ping) request ic	
	5 5.962414000	tsukumotan	emachine	ICMP	74 5.962747000	Echo (ping) reply		ICMP: Echo (ping) reply id:	
	6 5.962747000	emachine	tsukumotan	ICMP	74 6.968220000	Echo (ping) request		ICMP: Echo (ping) request ic	
	7 6.968220000	tsukumotan	emachine	ICMP	<sup>74</sup> 6.971476000	Echo (ping) reply		ICMP: Echo (ping) reply id:	
	8 6.971476000	emachine	tsukumotan	ICMP	74 7.974054000	Echo (ping) request		ICMP: Echo (ping) request ic	
	9 7.974054000	tsukumotan	emachine	ICMP	7/	Echo (ping) reply	100	" - '	
	10 7.974310000	emachine	tsukumotan	ICMP	74 7.974310000	(0)1(0)	1	ICMP: Echo (ping) reply id:	
	11 10.598752000	tsukumotan	Broadcast	ARP	47 10.600076000	Echo (ping) request	<b>→</b> (a)	ICMP: Echo (ping) request ic	
	12 10.600066000	viera	tsukumotan	ARP	6(10.602619000	Echo (ping) reply		ICMP: Echo (ping) reply id:	
	13 10.600076000	tsukumotan	viera	ICMP	74՝£ՀñԾ՝(Թիից) r	Faha (nina) request			
			and the same of th						

## 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)



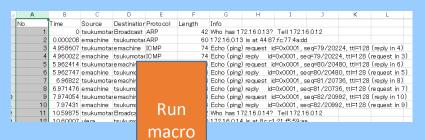
4	A	В	С	D	E	F	G	Н	I	J	K	L
1	No.	Time	Source	Destination	Protocol	Length	Info					
2	1		tsukumotar						? Tell 172.1			
3	2	0.000208	emachine	tsukumotar	ARP				37:fc:77:4a:d	-		
4	3	4.958607	tsukumotar	emachine	ICMP	74	Echo (ping					3 (reply in 4)
5	4		emachine				Echo (ping					(request in 3
6	5		tsukumotar									3 (reply in 6)
7	6	5.962747	emachine	tsukumotar	ICMP		Echo (ping					(request in 5
8	7	6.96822	tsukumotar	emachine	ICMP							3 (reply in 8)
9	8		emachine				Echo (ping					(request in 7
10	9		tsukumotar									3 (reply in 10)
11	10		emachine								2, ttl=128	(request in 9
12	11		tsukumotar	Broadcast	ARP				? Tell 172.1			
13	12	10.60007		tsukumotar					c1:21:f5:59:a			
14	13		tsukumotar		ICMP							3 (reply in 14)
15	14	10.60262		tsukumotar			Echo (ping					request in 13
16	15		tsukumotar		ICMP							3 (neply in 16)
17	16	11.60625		tsukumotar			Echo (ping					request in 15
18	17		tsukumotar		ICMP							3 (reply in 18)
19	18	12.61225		tsukumotar			Echo (ping					request in 17
20	19		tsukumotar		ICMP							3 (reply in 20)
21	20	13.62142		tsukumotar			Echo (ping				6, ttl=64 (	request in 19
22	21		Fortinet_bf:						? Tell 172.1			
23	22	15.59985	tsukumotar	Fortinet_bf:	ARP	42	172.16.0.12	2 is at 00:2	26:18:37:3a:5	0		
24												

#### Create some macros

4	Α	В	С	D	Е	F	G	Н	I	J	K	L
	No.	Time	Source	Destination	Protocol	Length	Info					
	1	0	tsukumotar	Broadcast	ARP	42	Who has 17	72.16.0.13?	Tell 172.1	6.0.12		
	2	0.000208	emachine	tsukumotar	ARP	60	172.16.0.13	l is at 44:8	7:fc:77:4a:dc			
	3	4.958607	tsukumotar	emachine	ICMP	74	Echo (ping)	request i	d=0x000 <mark>1</mark> , s	eq=79/202	24, ttl=128	(reply in 4)
	4	4.960022	emachine	tsukumotar	ICMP	74	Echo (ping)	reply id:	=0x0001, se	q=79/2022	4, ttl=128 (	request in 3)
	5	5.962414	tsukumotar	emachine	ICMP	74	Echo (ping)	request i	d=0x000 <mark>1</mark> , s	eq=80/204	80, ttl=128	(reply in 6)
	6	5.962747	emachine	tsukumotar	ICMP	74	Echo (ping)	reply id:	=0x0001, se	q=80/2048	0, ttl=128 (	request in 5)
	7	6.96822	tsukumotar	emachine	ICMP	74	Echo (ping)	request i	d=0x000 <mark>1</mark> , s	eq=81/207	36, ttl=128	(reply in 8)
	8	6.971476	emachine	tsukumotai	ICMP	74	Echo (ping)	reply id:	=0x0001 , se	q=81/2073	6, ttl=128 (	request in 7)
)	9	7.974054	tsukumotar	emachine	ICMP	74	Echo (ping)	request i	d=0x000 <mark>1</mark> , s	eq=82/209	92, ttl=128	(reply in 10)
	10	7.97431	emachine	tsukumotar	ICMP	74	Echo (ping)	reply id:	=0x000 <b>1</b> , se	q=82/2099	2, ttl=128 (	request in 9)
1	11	10.59875	tsukumotar	Broadcast	ARP	42	Who has 17	72.16.0.14?	Tell 172.1	6.0.12		
	12	1.0.60007	vie re	teukumotai	APP	60	17216014	ie at 8c·c	1-21-f5-59-55	1		

Sharkfest 2014

# Looking good? Handsome!!





1	Time	Source	Destination	Protocol	Length	Info							
3	0.000208	emachine	tsukumota	ARP	60	172.16.0.1	3 is at 44	l:87:fc:77:4a	i:dd	- 1	IME DU	RATION	
5		emachine	tsukumotai	ICMP		Echo (ping						(request in 3	
7	5.962747		tsukumota		74	Echo (ping	() reply	_id=0x0001 .	sea=80/	/20480	D. ttl=128	request in 5	5)
9	6.971476	emachine	tsukumota	ICMP	74	Echo (ping	r) reply	_id=0x0001 .	sea=81/	/20736	3. ttl=128 i	request in T	7)
11	7.97431	emachine	tsukumota	ICMP	74	Echo (ping	) reply	id=0x0001,	seq=82/	/20992	2, tt⊫128 I	(request in 9	9)
15	10.60262	l viera	Itsukumotai	ICMP	74	Echo (ping	r) reply	id=0x0001.	sea=83/	/21248	3. tt⊫64 (r	eauest in 13	3)
17	11.60625		tsukumota		74	Echo (ping	ne plv	id=0x0001.	sea=84/	/21504	4. ttl=64 (r	eauest in 15	5)
19	12.61225	viera	tsukumota	ICMP	74	Echo (ping	r) reply	_id=0x0001 .	sea=85/	/21760	D. ttl=64 (r	eauest in 17	7)
21	13.62142	? viera	tsukumotai	ICMP	74	Echo (ping	) reply	id=0x0001,	seq=86/	/22016	6, ttl=64 (r	equest in 19	9)
22	15.59983	Fortinet_bf	tsukumota	ARP	60	Who has 1	72.16.0.1	2? Tell 172	2.16.0.1				
23	15.59985	tsukumota	Fortinet_bf	ARP	42	172.16.0.13	2 is at 00	):26:18:37:38	a:50				
24			_										

Thank you

