### **Documentation d'installation**



Exportation audio d'une capture de trame RTP (SIP TrixBox)





28/03/2018



### Sommaire

1.	Qu'est-ce que la VOIP	3
2.	Capture de trames	3
3.	Ecoute des échanges audios	3
4.	Exportation trames RTP en version audio	6

# 1. Qu'est-ce que la VOIP

VOIP est un acronyme qui signifie "**Voice Over Internet Protocol**", ou en d'autres termes, la transmission de la voix via Internet. C'est une technologie qui permet de délivrer des communications vocales ou multimédia (vidéo par exemple) via le réseau TCP IP.

# 2. Capture de trames

Afin de pouvoir exporter notre conversation audio, nous devons enregistrer les trames échangées. Pour cela nous devons nous rendre sur WireShark, et sélectionner notre interface à écouter.

Pour ma part c'est "VMWare Network Adapter VMnet2", on le sélectionne.

L'analyseur de réseau Wireshark		- U	×
Fichier Editer Vue Aller Cap	ture Analyser Statistiques Telephonie Wireless Outils. Aide		
🖌 = 🦽 😔 📒 🗁 🛪 🖾 I	Q 🐵 🕫 😤 🚍 🔍 Q Q Q 표		
Appliquer un filtre d'affichage <cti< th=""><th>42</th><th>Expression</th><th>1 +</th></cti<>	42	Expression	1 +
	Bienvenue dans Wireshork		
	Capture		
	en utilizant ce filte 🖡 Renther un filtre de capture 👻 Al Interfaces aboun *		
	VMware Network Adapter VMnet2		
	VirtualBox Host-Only Network #3		
	VMware Network Adapter VMmet1		
	Chemet //		
	Automation Whatare Network & danster Whines A		
	USBPcap1		
	USBPcap2		
	© USEPcap3		

Normalement c'est l'interface "Ethernet", mais moi il s'agit de la carte réseau dédier à mes serveur Virtuelle

Une fois sélectionné, l'écoute commence et tout le trafic à destination de mon ordinateur est affiché.

Appliquer un fil	iltre d'afficha	ge <ctrl-></ctrl->			• Expression
Time		Source	Destination	Protocol	Length Info
25 8.77	78538	172.16.53.151	188.165.236.162	NTP	90 NTP Version 4, client
26 8.77	79030	172.16.53.151	129.250.35.250	NTP	90 NTP Version 4, client
27 8.79	90528	129.250.35.250	172.16.53.151	NTP	90 NTP Version 4, server
28 8.79	93056	188.165.236.162	172.16.53.151	NTP	90 NTP Version 4, server
29 10.6	663868	172.16.53.254	172.16.53.152	ICNP	84 Destination unreachable (Host unreachable)
30 10.6	663869				84 Destination unreachable (Host unreachable)
31 12.1	100846	Vmware_c0:00:02	Vmware_ef:5e:81	ARP	42 Who has 172.16.53.152? Tell 172.16.53.1
32 12.1	101627	Vmware_ef:Se:81	Vmware_c0:00:02	ARP	42 172.16.53.152 is at 00:0c:29:ef:5e:81
33 13.8	811639	Vmware_06:2d:f4	Vmware_88:13:05	ARP	60 Who has 172.16.53.151? Tell 172.16.53.254
34 13.8	812848	Vmware_88:13:05	Vmware_06:2d:f4	ARP	42 172.16.53.151 is at 00:0c:29:88:13:05
35 14.1	129254	Vmware_88:13:05	Broadcast	ARP	42 Who has 172.16.53.100? Tell 172.16.53.151
36 14.1	130225	Vmware_27:16:e6	Vmware_88:13:05	ARP	42 172.16.53.100 is at 00:0c:29:27:16:e5
37 14.1	131228	172.16.53.151	172.16.53.100	DNS	81 Standard query 0x2481 A trixbox1.freshome.lan
38 14.1	132517	172.16.53.100	172.16.53.151	DNS	130 Standard guery response 0x2481 A trixbox1.freshome.lan A 172.16.53.151 NS ns.freshome.lan A 172.16.53.100
39 17.2	282866	172.16.53.1	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
40 18.2	283504	172.16.53.1	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
41 19.2	283685	172.16.53.1	239.255.255.250	SSDP	216 M-SEARCH * MTTP/1.1
42 19.3	398954	Vmware_27:16:e6	Vmware_88:13:05	ARP	42 Who has 172.16.53.1517 Tell 172.16.53.100
43 19.3	391593	Vmware_88:13:05	Vmware_27:16:e6	ARP	42 172.16.53.151 is at 00:0c:29:88:13:05
44 28.2	284398	172.16.53.1	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
45 27.7	713238	172.16.53.152	192.168.1.1	IAX2	S6 IAX, source call# 1591, timestamp 17ms POKE
46 28.8	846991	172.16.53.1	172.16.53.100	DNS	84 Standard query 0xe542 A notifications.google.com
47 28.8	848211	172.16.53.100	216.239.38.10	DNS	77 Standard query 0x4e67 A plus.l.google.com
48 28.0	063944	216.239.38.10	172.16.53.100	DNS	93 Standard query response 0x4e67 A plus.l.google.com A 172.217.18.206
49 28.8	865215	172.16.53.100	172.16.53.1	DNS	369 Standard query response 0xe542 A notifications.google.com CNAME plus.l.google.com A 172.217.18.206 NS ns2.google.com NS ns4.google.com NS ns3.google.com NS ns1.google.com A 216.239.32.10
50 28.7	724412	172.16.53.152	192.168.1.1	IAX2	56 IAX, source call# 1591, timestamp 17ms POKE
51 29.6	644396	172.16.53.1	172.16.53.152	SIP/SDP	1427 Request: INVITE sip:100172.16.53.152
52 29.6	647589	172.16.53.152	172.16.53.1	SIP	618 Status: 401 Unauthorized
53 29.6	648487	172.16.53.1	172.16.53.152	SIP	390 Request: ACK sip:10@172.16.53.152
54 29.6	652937	172.16.53.1	172.16.53.152	IPv4	1514 Fragmented IP protocol (proto-UDP 17, off-0, ID-756f) [Reassembled in #55]
55 29.6	652944	172.16.53.1	172.16.53.152	SIP/SDP	85 Request: INVITE sip:100172.16.53.152
56 29.6	655579	172.16.53.152	172.16.53.1	SIP	554 Status: 100 Trying
57 29.6	686105	Vmware_ef:5e:81	Broadcast	ARP	42 Who has 172.16.53.100? Tell 172.16.53.152
52 20 F	627000	Vewane 27:16:66	Umiano of Soisi	100	43 177 16 52 100 is at 00.0c.30.37.16.06

# 0000 0100 00000 00000 00000 00000 00000

Maintenant, nous pouvons effectuer l'appelle SIP. Cela fonctionne de SIP > Serveur > SIP et normalement aussi de SIP > SIP.

# 3. Ecoute des échanges audios

Une fois notre écoute lancée, nous avons nos trames RTP qui sont parmi toutes nos trames

Droffi Dofau

appelle 2.pcaping				-	a ×
Fichier Editer Vue Aller Capture	Analyser Statistiques	Telephonie	Wireless Outils. Aide		
	++ = T + = =		3. 罪		
Anniaus un filme d'affichance - «Chi./»			-	<b>-</b>	Everanico
A population of the contracting and starting	Real Sector	0 - to - 1	1		Copi Coordina.
1 0 172 16 30 17	230 255 255 250	SCRD	Lengtr Jmt 3 70 MCEADCH * MTTD/3 3		
2 0 172.16.53.1	172.16.53.20	TPKT	139 Continuation		
3 0 172.16.53.20	172.16.53.1	TCP	54 10561 + 3389 [ACK] Seg=1 Ack=86 Win=2052 Len=0		
			60 Conf. Root = 32768/0/68:af:67:2c:75:0d Cost = 39 Port = 0x8803		
5 1 172.16.53.1	172.16.53.20	TPKT	139 Continuation		
6 1 172.16.53.20	172.16.53.1	TCP	54 10561 + 3389 [ACK] Seq=1 Ack=171 Win=2052 Len=0		
7 2 172.16.53.1	172.16.53.20	TPKT	139 Continuation		
8 2 172.16.53.20	172.16.53.1	TCP	54 10561 + 3389 [ACK] Seq=1 Ack=256 Win=2052 Len=0		
9 2 172.16.53.101	172.16.53.100	DNS	80 Standard query 0x31b1 A fe2.ws.microsoft.com		
10 2 172.16.53.20	1/2.16.20.1	UNS	80 Standard query exable ARAA clients.1.google.com		
11 2 1/2.16.28.1	1/2.16.53.20	UNS THE	ide standard query response exable AAAA clients.1.google.com AAAA 200014501400/18001200e		
12 2 1/2.10.55.20	210.50.200.250	TLSVI.2	so 4 application bats		
15 2 210.50.200.250	Snanning-tree-(for-	STP	00 445 7 10540 [AKK] SCH1 ACK-001 ALI-SCT COMMO		
15 2 CiscoInc 33:09:83	CiscoInc 33:09:83	LOOP	60 Reply		
16 2 216,58,208,238	172.16.53.20	TLSv1.2	462 Application Data, Application Data, Application Data		
17 2 172.16.53.20	216.58.208.238	TLSv1.2	100 Application Data		
18 2 216.58.208.238	172.16.53.20	TCP	60 443 → 10946 [ACK] Seq=409 Ack=547 Win=512 Len=0		
19 2 172.16.53.20	216.58.208.238	TLSv1.2	1142 Application Data		
20 2 216.58.208.238	172.16.53.20	TCP	60 443 → 10860 [ACK] Seq=1 Ack=1089 Win=504 Len=0		
21 2 172.16.53.20	172.16.53.3	TCP	66 10979 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1		
22 2 172.16.53.3	172.16.53.20	TCP	66 80 + 10979 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128		
23 2 172.16.53.20	172.16.53.3	TCP	54 10979 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0		
<ul> <li>Frame 1: 179 bytes on wire (1</li> <li>Ethernet II, Src: HewlettP_7c</li> <li>Internet Protocol Version 4,</li> <li>User Datagram Protocol, Src P</li> </ul>	<pre>case = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 =</pre>	eaptured (. 9:db), Dst t: 239.255 st Port: 19	%2∠015) on Inferface 0 Th¥eacat_71fifa (01100:5e:7fiffifa) 255.750 00 (1900)		Í
0000         0100         50         7 ff ff h db         aff           000         7 ff ff h db         80         80         10         00         57           0000         7 ff ff h db         80         80         10	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00			
0 2				Paquets: 3954 · Affichés: 3954 (100.0%)· Temps de chargement: 0:0.103	Profil: Defau

Une fois que nous avons toutes nos trames, nous allons cliquer sur "**Telephonie**", puis sur "**RTP**" et pour finir "**RTP Streams**".

	≈ ∞ ≚ ∎ ⊻ [⊒]	VOIP Calls	
:Ctrl-/>		ANSI	
	Destination	GSM •	
	239.255.255.250	IAX2 Stream Analysis HTTP,	/1.1
	172.16.53.20 172.16.53.1	Messages ISUP 9 [A0	[K] Seq=1 Ack=86 Win=2052 Len=0
a9:83	Spanning-tree-(for 172.16.53.20	MTP3 = 32	768/0/b8:af:67:2c:75:0d
	172.16.53.1	RTP P	TP Streams /1 Win=2052 Len=0
	172.16.53.20 172.16.53.1	RTSP	Stream Analysis 56 Win=2052 Len=0
1	172.16.53.100 172.16.20.1 172.16.53.20 216.58.208.238	SCTP ery of Opérations SMPP ery of Messages UCP ery of Data	0x31b1 A fe2.ws.microsoft.com 0xab1e AAAA clients.l.google.com response 0xab1e AAAA clients.l.goo a
38	172.16.53.20	H.225	<pre>{] Seg=1 Ack=501 Win=509 Len=0</pre>
39:83	Spanning-tree-(for	SIP Flows = 32	768/0/b8:af:67:2c:75:0d Cost = 39
29:83	CiscoInc_33:09:83	SIP Statistics	
38	172.16.53.20 216.58.208.238	WAP-WSP Packet Counter Data	a, Application Data, Application D a
38	172.16.53.20 216.58.208.238	TCP         60 443 → 10946         [ACI           TLSv1.2         1142 Application Data	<pre>(] Seq=409 Ack=547 Win=512 Len=0 a</pre>
38	172.16.53.20	TCP 60 443 → 10860 [AC	(] Seg=1 Ack=1089 Win=504 Len=0

Cela peut varier dans les anciennes versions de WireShark

Nous avons maintenant une fenêtre qui s'ouvre et nous devons sélectionner nos flux qui ont été détectés.

Nous allons sélectionner les 2 flux bleus, ce qui nous permettra d'avoir la conversation entière. Il est possible de sélectionner qu'1 seul flux ce qui a pour effet, d'entendre uniquement l'utilisateur 1 ou l'utilisateur 2. En sélectionnant les 2, on a donc les deux utilisateurs superposés qui recompose l'appel.

Wireshark - RT	TP Streams · ap	pelle 2															-		×
Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Paquets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Etat								1
172.16.53.101	11394	172.16.53.20	5096	0x234a7678	h263	803	0 (0.0%)	0.000	0.000	0.000									_
172.16.53.101	19724	172.16.53.20	5094	0x62bf841	g711U	1324	0 (0.0%)	27.182	1.635	0.754									
172.16.53.20	5094	172.16.53.101	19724	0x3fef0aaf	q711U	1261	0 (0.0%)	21.628	1.105	0.662									
3 streams. Right-click :	for more options.																_		
												Close	Find Reverse	Prepare Filter	Export	Copier 🔻	Analyse	He	þ

Une fois sélectionné, nous devons les analyser pour cela cliquer sur "Analyse"

Wireshark - RT	'P Streams · ap	pelle 2															<u>19</u> 2		×
Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Paquets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Etat								
172.16.53.101	11394	172.16.53.20	5096	0x234a7678	h263	803	0 (0.0%)	0.000	0.000	0.000									
172.16.53.101	19724	172.16.53.20	5094	0x62bf841	g711U	1324	0 (0.0%)	27.182	1.635	0.754									
172.16.53.20	5094	172.16.53.101	19724	0x3fef0aaf	g711U	1261	0 (0.0%)	21.628	1.105	0.662									
3 streams, 2 selected,	2585 total packets	s. Right-click for more options										Close	Find Reverse	Prepare Filter	Export	Copier 🔻	Analyse	Hel	p

#### Une fois analysé, nous avons le détail de l'échange. Cliquer sur "Play Streams" pour écouter

Wireshark · KIP Stream A	Analysis · appe	lle 2							<u>8</u>	
2.16.53.101:19724 ↔	Forwar	d Revers	e Graphiq	ue						
2.10.33.20.303 1	Paquet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bande passante	Marker	tat		
orward	220	23978	0.00	0.00	0.00	1.60				
Dv062bf841	223	23979	19.86	0.00	0.14	3.20	1999			
ax Delta 27.18 ms @ 16	15 220	22080	21.07	0.08	-0.94	4.80				
x Jitter 1.64 ms	231	23081	10.03	0.00	-0.87	6.40				
an Jitter 0.75 ms	23/	22092	20.10	0.08	-1.06	8.00				
ax Skew -8.38 ms	236	23082	20.15	0.00	-1 00	9.60				
P Packets 1324	240	22004	20.35	0.14	-2.25	11.00				
pected 1324	240	22004	10.02	0.14	-2.19	12.20				
st 0 (0.00 %)	245	23303	20.64	0.14	-2.02	14.40				
q Errs 0	245	23500	20.04	0.17	-2.02	14,40				
vok Drift -787 mg	240	23507	10.04	0.10	2.05	17.60				
eg Drift 7913 Hz (-1.08	%) 257	20000	19.94	0.10	-2.05	17.00				
	252	23989	20.14	0.72	6.30	19.20				
verse	200	22001	20.14	0.09	0.22	20.60				
	257	23991	20.12	0.00	0.10	22.40				
KC 0X00201041	200	23992	20.92	0.07	5.18	24.00				
vlitter 1 10 ms	203	23993	20.40	0.65	4.77	25.60				
an Jitter 0.66 ms	265	23994	20.54	0.64	4.23	27.20				
ax Skew 6.81 ms	268	23995	20.43	0.63	3.80	28.80				
P Packets 1261	270	23996	20.22	0.60	3.58	30.40				
pected 1261	2/4	23997	20.18	0.58	3.40	32.00				
st 0 (0.00 %)	277	23998	20.60	0.58	2.80	33.60				
eq Errs 0	280	23999	20.36	0.57	2.44	35.20				
iration 25.19 s	283	24000	20.59	0.57	1.85	36.80				
en Drift 7902 Hz ( 1 22	285	24001	19.68	0.55	2.17	38.40				
req Drift 7902 Hz (-1.22	288	24002	20.45	0.55	1.72	40.00				



Nous avons la recomposition de notre échange que nous pouvons écouter grâce au bouton "▶"

### 4. Exportation trames RTP en version audio

Une fois que nous avons nos trames il est possible de les exporter au format audio, pour cela nous devons revenir à la page d'avant et cliquer sur "**Save**", puis "**Audio**".

172.16.53.10	1:19724 ↔	Forward	Bewerren	Graphia	10									
172.16.53.20	5094	Desurt	Converse	Dalta (ma)	litter (mar)	Cherry	Danala anaraka	Manhan	[ test					•
Forward		220	23079	0.00	Jitter (ms)	0.00	bande passante	Warker	Eldi					
SSDC	0x062bf841	223	23979	19.86	0.01	0.14	3.20							-
Max Delta	27.18 ms @ 1615	220	23080	21.07	0.08	-0.94	4 80							
Max litter	1.64ms	221	12001	10.02	0.07	-0.97	5.40							
Mean Jitter	0.75 ms	224	22002	20.10	0.00	-1.06	0.40							
Max Skew	-8.38 ms	126	23502	20.15	0.00	1.00	0.00							
<b>RTP</b> Packet	<b>s</b> 1324	230	23983	20.93	0.14	-1.99	9.00							
Expected	1324	240	23984	20.26	0.14	-2.25	11.20		~					
Lost	0 (0.00 %)	243	23985	19.93	0.14	-2.18	12.80		1					
Seq Errs	0	245	23986	20.64	0.17	-2.82	14.40		1					
Duration	26.45 s	248	23987	20.06	0.16	-2.89	16.00		1					
Clock Drift	-287 ms	251	23988	19.94	0.16	-2.83	17.60		1					
Freq Drift	/913 Hz (-1.08 %)	252	23989	10.81	0.72	6.36	19.20		1					
Reverse		255	23990	20.14	0.69	6.22	20.80		1					
increase.		257	23991	20.12	0.65	6.10	22.40		1					
SSRC	0x062bf841	260	23992	20.92	0.67	5.18	24.00		1					
Max Delta	21.63 ms @ 1493	263	23993	20.40	0.65	4.77	25.60		1					
Max Jitter	1.10 ms	265	23994	20.54	0.64	4.23	27.20		1					
Mean Jitter	0.66 ms	268	23995	20.43	0.63	3.80	28.80							
Max Skew	6.81 ms	270	23006	20.22	0.60	3 58	30.40							
RTP Packet	\$ 1261	274	12007	20.19	0.50	2.40	22.00							
Expected	1261	277	23997	20.00	0.50	3.40	32.00							
Lost	0 (0.00 %)	200	23990	20.00	0.50	2.00	55.00							
Seq Errs	0	280	23999	20.30	0.57	2.44	35.20							
Cleak Drift	20.195	283	24000	20.59	0.57	1.85	30.80		1					
Erea Drift	7907 Hr (-1 72 %)	285	24001	19.68	0.55	2.17	38.40		1					100
ineq bine	7302112 (11.22 76)	288	24002	20.45	0.55	1.72	40.00	1	1					~
2 streams found														
											Save  Close Pla	y Streams	Help	
											Audio	_	_	_
s.											Forward Stream Audio			
										Close	Reverse Stream Audio	oct	Copier	-
											Reverse stream Addie		copiei	
											CSV			
											Forward Stream CSV			
											romand stream CSV			
											CT C			

Une fois fait, nous pouvons donc l'exporter, il peut être lu par "Audacity"

<u>N</u> om du fichier :	Saved RTP Audio	~
Ţype :	Sun Audio (*.au)	×
∧ Masquer les dossi	ers	Enregistrer Annuler