

**Institut Universitaire de Technologie,
Aix-Marseille Université**

**ANNEXES
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications**

**Stage au sein du pôle technique télécoms et
réseaux d'EDF**

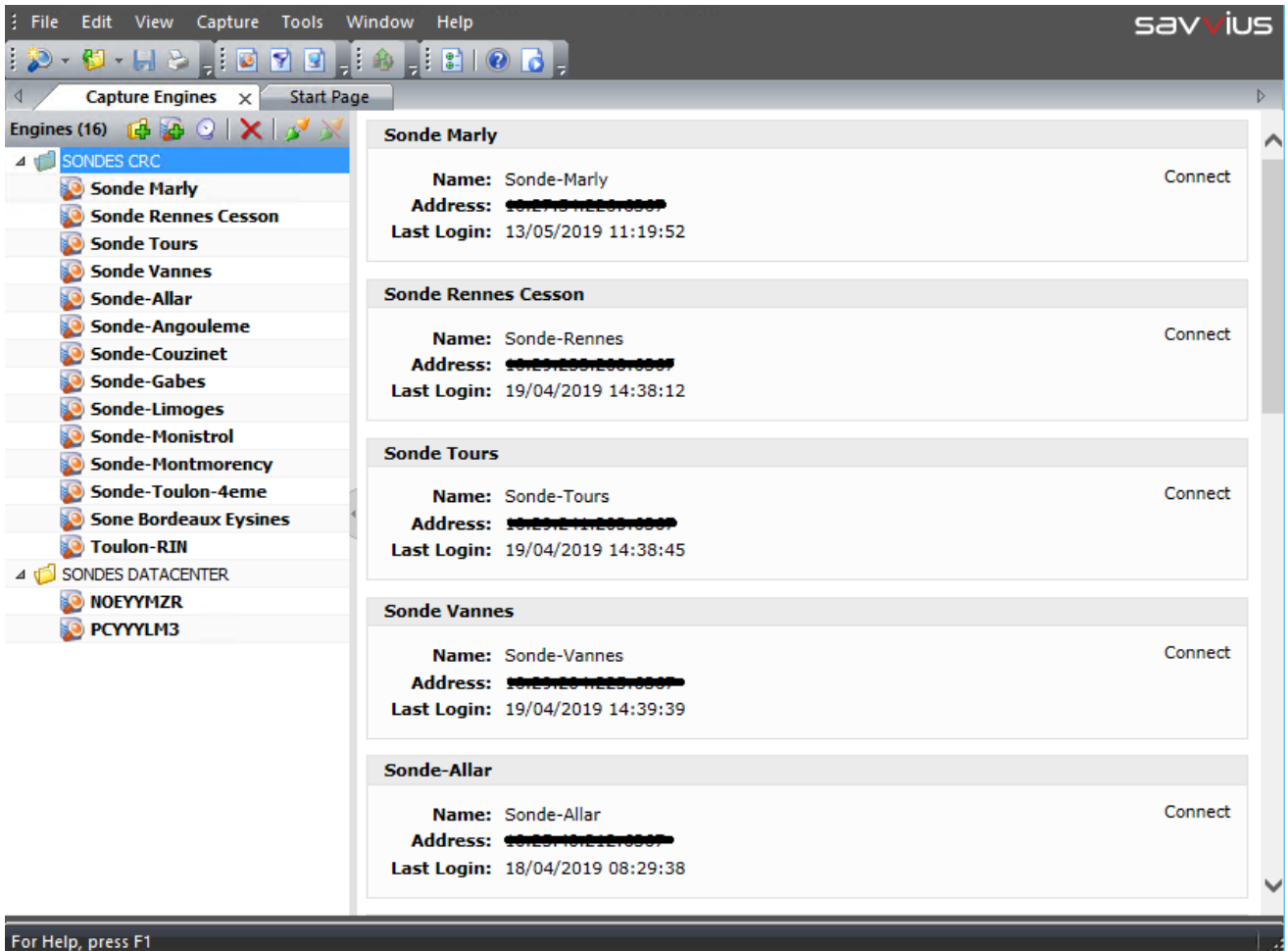
Thomas RICHARD

EDF

Responsable entreprise : Thomas REUTENAUER

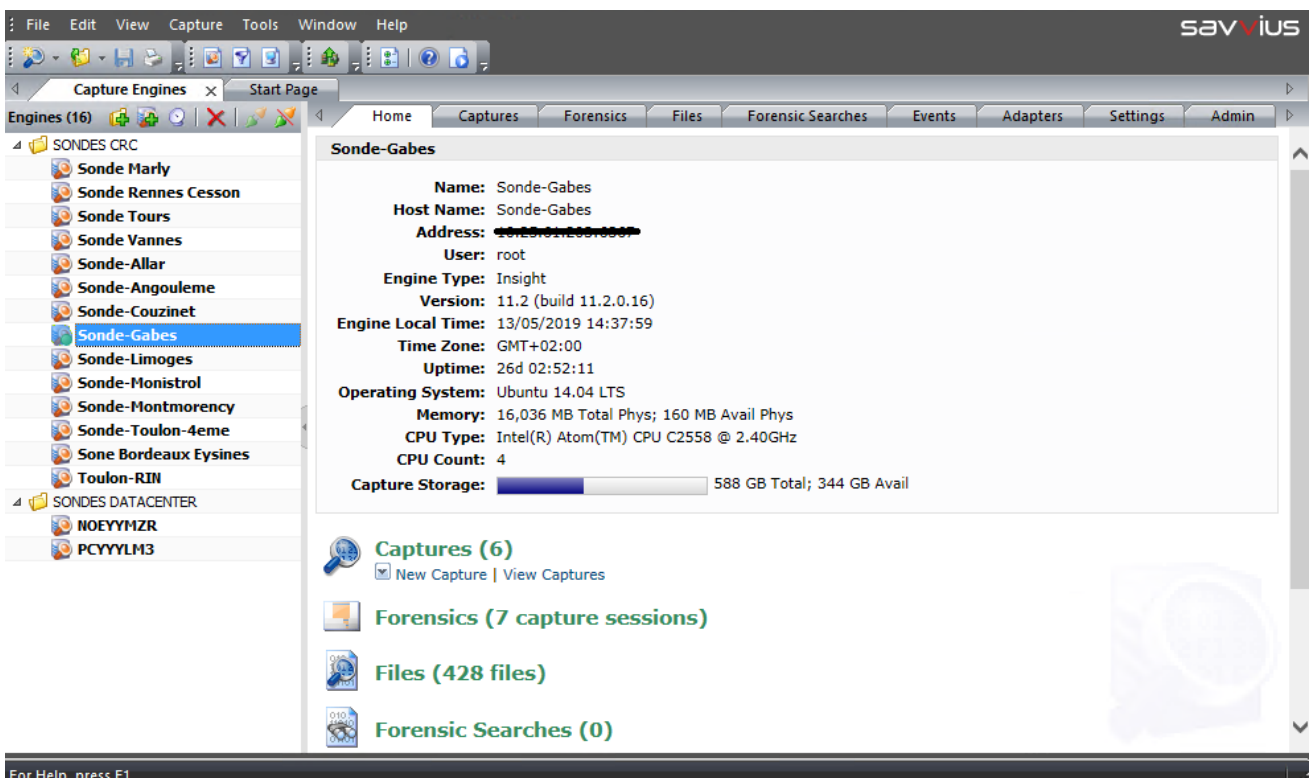
Responsable académique : Éric SOCCORSI

2019



Annexe 1 : Liste des sondes dans l'onglet « Capture Engines » sur OmniPeek.

On peut se connecter aux sondes avec un identifiant et un mot de passe en cliquant sur « Connect »



Annexe 2 : Information relatives a la sonde de Marseille Gabès

Alarm	Suspect Condition	Problem Condition	Created	Modified
802.11 Retry	> 1/s for 5 seconds	> 1/s for 10 seconds	05/02/2009 21:28:09	05/02/2009 21:28:09
ARP Requests	> 1/s for 10 seconds	> 3/s for 5 seconds	15/10/2003 00:13:36	15/10/2003 00:13:36
Average Utilization (percent)	> 50/s for 5 seconds	> 75/s for 5 seconds	01/11/2004 23:36:51	01/11/2004 23:36:51
Charge PA RIN critique - 80%	> 4000000/s for 60 seconds		18/04/2019 09:56:43	19/04/2019 15:36:34
CRC Errors	> 2/s for 1 seconds	> 2/s for 5 seconds	15/10/2003 00:04:29	15/10/2003 00:04:29
Current Utilization (%)	> 60 for 5 seconds	> 75 for 5 seconds	16/10/2003 01:47:34	16/10/2003 01:47:34
DECnet Addresses Seen	> 1/s for 1 seconds	> 10/s for 1 seconds	15/10/2003 00:05:39	15/10/2003 00:05:39
Errors Total	> 2/s for 3 seconds	> 2/s for 7 seconds	15/10/2003 00:03:40	15/10/2003 00:03:40
Excessive 802.11 management traffic	> 30/s for 5 seconds	> 50/s for 3 seconds	05/02/2009 21:29:11	05/02/2009 21:59:57
Excessive Minimum Data Rate Packets	> 30/s for 5 seconds	> 30/s for 10 seconds	05/02/2009 21:36:53	05/02/2009 21:36:53
Frame Alignment	> 1 for 1 seconds	> 3 for 1 seconds	02/11/2004 00:17:37	02/11/2004 00:18:24
FTP Failed Transfers	> 1/s for 1 seconds	> 5/s for 1 seconds	15/10/2003 00:07:02	15/10/2003 00:07:02
FTP Successful Transfers	> 1/s for 5 seconds	> 2/s for 5 seconds	01/11/2004 23:40:14	01/11/2004 23:40:14
FTP Transfers Initiated	> 1/s for 5 seconds	> 2/s for 5 seconds	01/11/2004 23:40:40	01/11/2004 23:40:40
ICMP Addr Mask Req	> 1/s for 1 seconds	> 10/s for 1 seconds	14/10/2003 23:49:37	14/10/2003 23:49:37
ICMP Addr Mask Rsp	> 1 for 1 seconds	> 10 for 1 seconds	01/11/2004 23:41:31	01/11/2004 23:41:31
ICMP Comm Prohibited	> 1 for 1 seconds	> 10 for 1 seconds	01/11/2004 23:43:03	01/11/2004 23:43:03

Annexe 3 : Liste de toutes les alarmes présentes sur la sonde de Marseille Gabès.

On peut voir celle que j'avais créer pour le système d'alertes par mail.

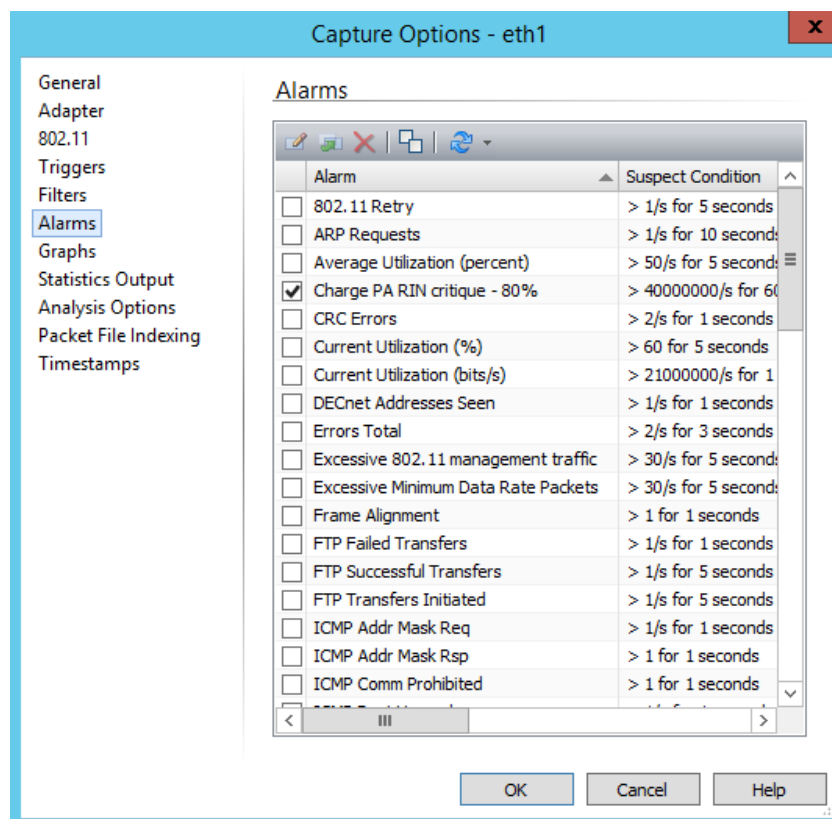
Statistic	Packets	Bytes	Value
General			
Start Date			19/04/2019
Start Time			16:30:12
Duration			33d 19:22:53.0...
Trigger Count			0
Trigger Wait Time			0.000000
Dropped Packets			0
Duplicate Packets Discarded			0
Network			
Total Bytes			3,282,658,652,...
Total Packets	6,303,726,644		
Total Broadcast	132	8,448	
Total Multicast	146,371	58,427,992	
Average Utilization (percent)			0.913
Average Utilization (bits/s)			9,128,706
Current Utilization (percent)			1.299
Current Utilization (bits/s)			12,991,520

Annexe 4 : Liste de toutes les statistiques relatives à la capture.

Pour créer une alarme il suffit de faire un clic droit sur la statistique que l'on veut surveiller puis sélectionner « Make Alarm ».

Nom du site	Bande passante disponible (en Mbit/s)	80% de la bande passante disponible (en Mbit/s)
Marly	50	40
Rennes Cesson	100	80
Tours	100	80
Vannes	30	24
Allar	100	80
Angoulême	30	24
Couzinet	50	40
Gabès	50	40
Limoges	30	24
Ministrol	20	16
Montmorency	50	40
Toulon	50	40
Bordeaux Eysines	50	40

Annexe 5 : Tableau rassemblant toutes les sondes avec leur bande passante disponible ainsi que 80% de la valeur de cette bande passante.



Annexe 6 : Onglet « Alarms » dans les options de captures qui permet d'activer une ou plusieurs alarmes.

On voit une seule alarme active pour cette capture.

Date	Time	Event
05/06/2019	09:57:11	Capture "Capture OTC Marly" options changed, Comment: "Capture sonde Marly"
05/06/2019	09:57:16	Capture "Capture OTC Marly" started
05/06/2019	09:57:16	Capture "Capture OTC Marly" started
05/06/2019	09:57:16	Capture "Capture OTC Marly" started
12/06/2019	08:46:05	Reset Alarm Event: Charge PA RIN critique - 80%
12/06/2019	09:09:04	Capture "Capture OTC Marly" stopped
12/06/2019	09:09:05	Capture "Capture OTC Marly" options changed, Comment: "Capture sonde Marly"
12/06/2019	09:09:10	Capture "Capture OTC Marly" stopped
12/06/2019	09:09:11	Capture "Capture OTC Marly" options changed, Comment: "Capture sonde Marly"
12/06/2019	09:09:20	Capture "Capture OTC Marly" stopped
12/06/2019	09:09:25	Capture "Capture OTC Marly" options changed, Comment: "Capture sonde Marly"
12/06/2019	09:09:27	Capture "Capture OTC Marly" started
12/06/2019	09:09:27	Capture "Capture OTC Marly" started
12/06/2019	16:10:46	Problem Event: Charge PA RIN critique - 80% (>40000000 for 60 seconds)
12/06/2019	16:15:59	Resolve Event: Charge PA RIN critique - 80% (<40000000 for 60 seconds)
12/06/2019	19:11:33	Problem Event: Charge PA RIN critique - 80% (>40000000 for 60 seconds)
12/06/2019	19:15:37	Resolve Event: Charge PA RIN critique - 80% (<40000000 for 60 seconds)
13/06/2019	08:11:13	Reset Alarm Event: Charge PA RIN critique - 80%
13/06/2019	08:11:13	Capture "Capture OTC Marly" stopped
13/06/2019	08:11:13	Capture "Capture OTC Marly" options changed, Comment: "Capture sonde Marly"
13/06/2019	08:12:23	Capture "Capture OTC Marly" stopped
13/06/2019	08:12:31	Capture "Capture OTC Marly" options changed, Comment: "Capture sonde Marly"
13/06/2019	08:12:34	Capture "Capture OTC Marly" started
13/06/2019	08:19:58	Reset Alarm Event: Charge PA RIN critique - 80%
13/06/2019	08:20:02	Capture "Capture OTC Marly" stopped
13/06/2019	08:20:08	Capture "Capture OTC Marly" options changed, Comment: "Capture sonde Marly"
13/06/2019	08:20:09	Capture "Capture OTC Marly" started

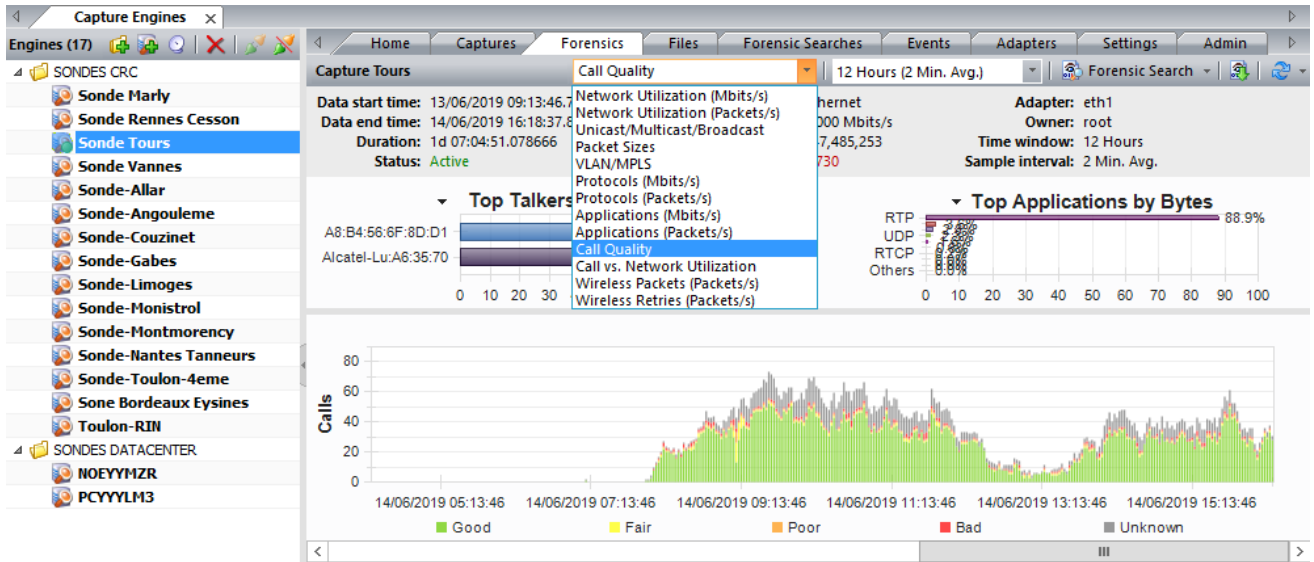
Annexe 7 : Onglet « Event » permettant de répertorier tous les Event d'une sonde (Exemple prit sur la sonde de Marly).

On peut voir qu'une alarme s'est activé deux fois et s'est résolue grâce au pictogramme jaune.

Home	Captures	Forensics	Files	Forensic Searches	Events	Adapters	Settings	Admin
Filters	Graphs	Alarms	Notifications	Protocol Translations	Trust Table	Analysis Modules	<input checked="" type="checkbox"/> Insert	
Actions (2)								
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Action				
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Log				
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Seuil d'utilisation 80% est dépassé				

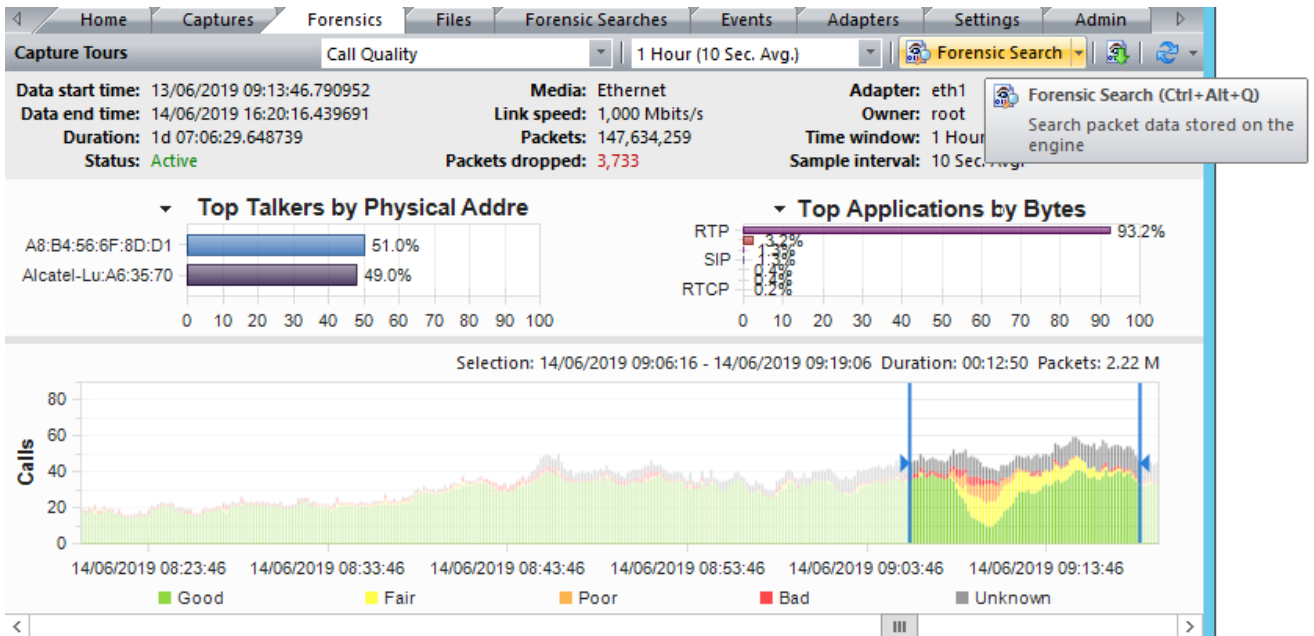
Annexe 8 : Onglet « Notification » permettant de gérer les actions présentes sur une sonde.

On peut voir le bouton « Insert » entouré en rouge permettant de créer une nouvelle action, on voit aussi que les deux cases à gauche qu'il faut cocher.



Annexe 9 : Onglet « Forensics » permettant d’observer l’évolution du MOS en temps réel.

On observe plusieurs petits pics rouges sur le haut du graphique car on ne peut pas garantir que 100% les appels vont bien se passer.



Annexe 10 : Sélection d’une zone du graphique pour lancer une « recherche forensic »

La sélection sur le graphique se fait simplement avec la souris et permet de faire une recherche sur un espace de temps précis.