Worcester Polytechnic Institute
Department of Computer Science

Module 2: Xplico analysis without ground truth

Objectives

- Use Xplico to examine the pcap files

Tasks

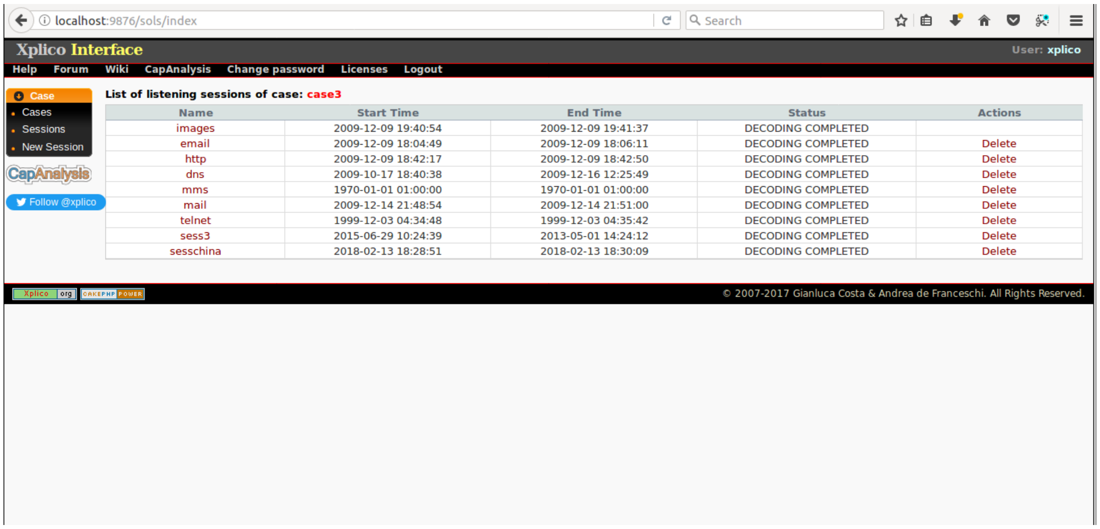
Step1: Create a case

1. On the Xplico interface, click on new case
2. Select 'Uploading pcap capture files' and provide case name as 'case 3' and click on create
3. New case is successfully created
4. Click on Case 3

Step 2: Create a session

1. In case 3, click on new session
2. Provide session name as below
3. Next, upload the pcap files. click browse. Select the pcaps file generated. Sample pcap files can be found here https://wiki.xplico.org/doku.php?id=pcap:pcap
4. Click upload and wait until the file is decoded
5. Next, after successful decoding, click hosts dropdown and select 'view all hosts' and click filter

For example, below are sessions created for different pcap files used



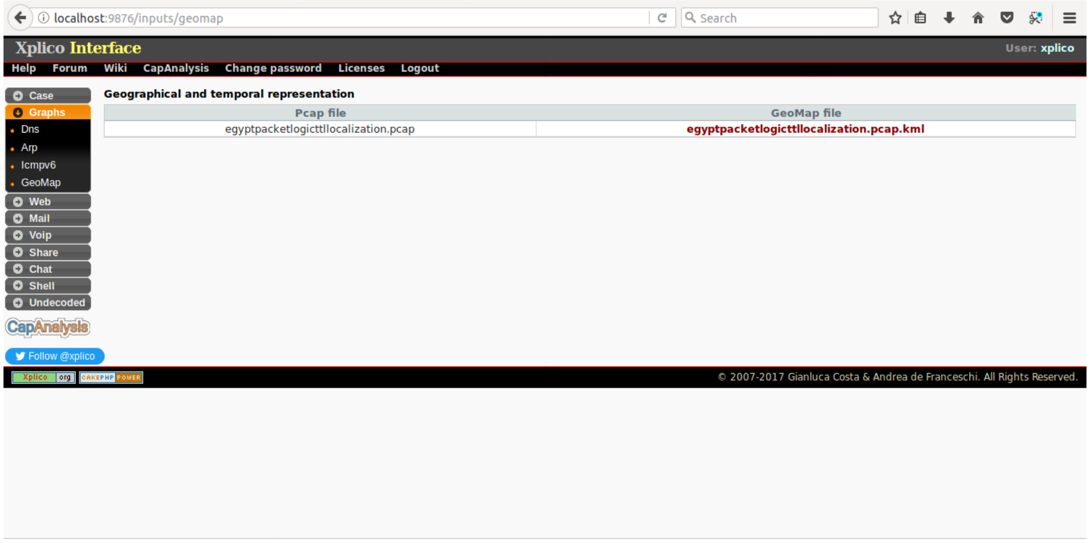
List of listening sessions of case: case3

Name	Start Time	End Time	Status	Actions
images	2009-12-09 19:40:54	2009-12-09 19:41:37	DECODING COMPLETED	
email	2009-12-09 18:04:49	2009-12-09 18:06:11	DECODING COMPLETED	Delete
http	2009-12-09 18:42:17	2009-12-09 18:42:50	DECODING COMPLETED	Delete
dns	2009-10-17 18:40:38	2009-12-16 12:25:49	DECODING COMPLETED	Delete
mms	1970-01-01 01:00:00	1970-01-01 01:00:00	DECODING COMPLETED	Delete
mail	2009-12-14 21:48:54	2009-12-14 21:51:00	DECODING COMPLETED	Delete
telnet	1999-12-03 04:34:48	1999-12-03 04:35:42	DECODING COMPLETED	Delete
sess3	2015-06-29 10:24:39	2013-05-01 14:24:12	DECODING COMPLETED	Delete
sesschina	2018-02-13 18:28:51	2018-02-13 18:30:09	DECODING COMPLETED	Delete

© 2007-2017 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Step 3: Analyze each pcap file

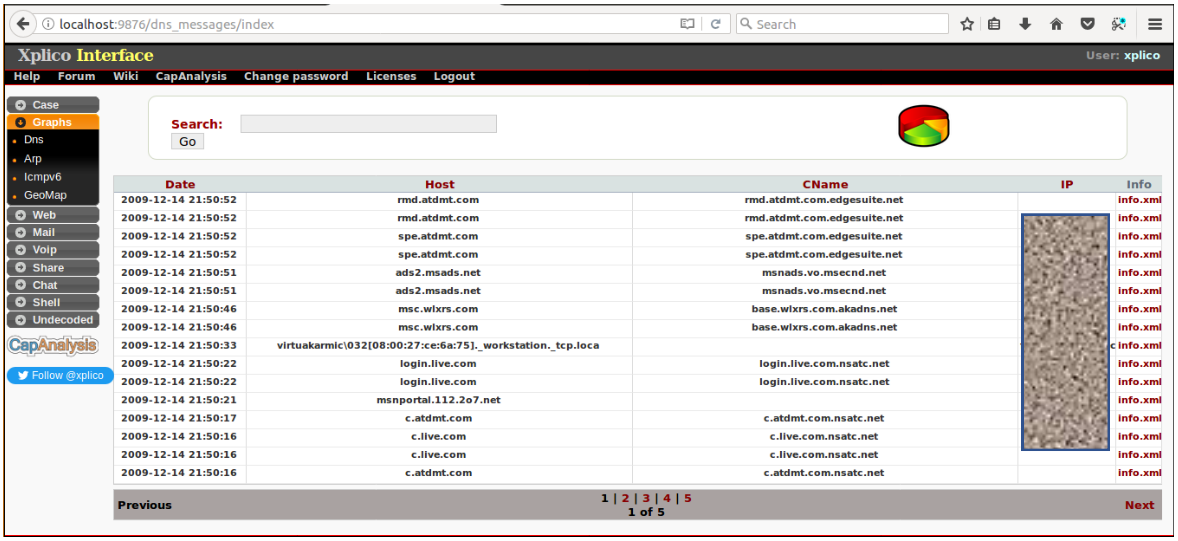
1. **GeoMap:** During a session decoding Xplico produces a KML file, this file, used with Google Earth, allows you to have a temporal and geographical map of connections decoded by Xplico.



Geographical and temporal representation

Pcap file	GeoMap file
egyptpacketlogicttllocalization.pcap	egyptpacketlogicttllocalization.pcap.kml

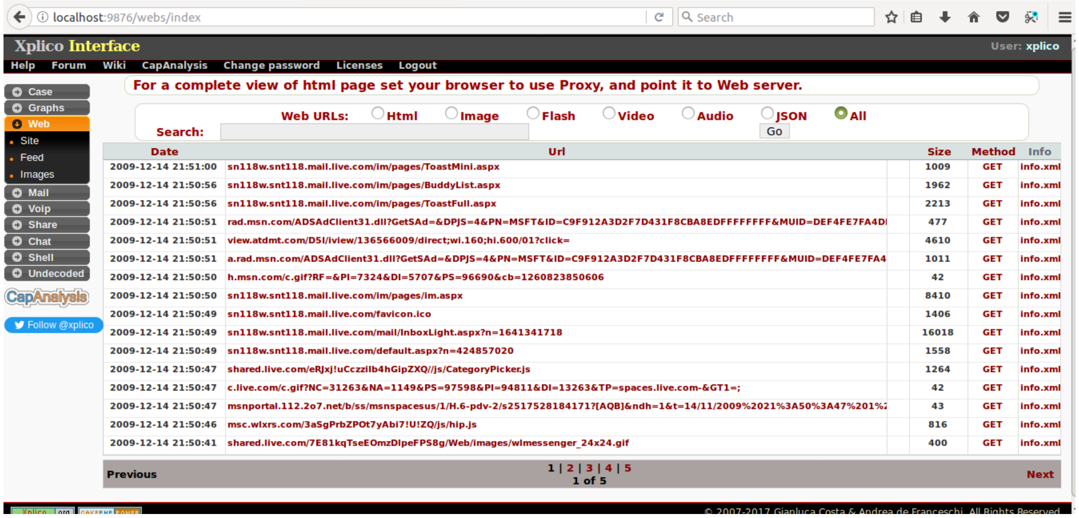
2. **DNS:** The DNS page displays all the DNS responses without error, listing the Canonical name if it exists and the first IP of response. Again, you can do research or to host or IP.



Date	Host	CName	IP	Info
2009-12-14 21:50:52	rmd.atdmt.com	rmd.atdmt.com.edgesuite.net		info.xml
2009-12-14 21:50:52	rmd.atdmt.com	rmd.atdmt.com.edgesuite.net	[redacted]	info.xml
2009-12-14 21:50:52	spe.atdmt.com	spe.atdmt.com.edgesuite.net	[redacted]	info.xml
2009-12-14 21:50:52	spe.atdmt.com	spe.atdmt.com.edgesuite.net	[redacted]	info.xml
2009-12-14 21:50:51	ads2.msads.net	msnads.vo.msecnd.net	[redacted]	info.xml
2009-12-14 21:50:51	ads2.msads.net	msnads.vo.msecnd.net	[redacted]	info.xml
2009-12-14 21:50:46	msc.wlxrs.com	base.wlxrs.com.akadns.net	[redacted]	info.xml
2009-12-14 21:50:46	msc.wlxrs.com	base.wlxrs.com.akadns.net	[redacted]	info.xml
2009-12-14 21:50:33	virtuakarmic\032[08:00:27:ce:6a:75]._workstation._tcp.loca		[redacted]	info.xml
2009-12-14 21:50:22	login.live.com	login.live.com.nsatc.net	[redacted]	info.xml
2009-12-14 21:50:22	login.live.com	login.live.com.nsatc.net	[redacted]	info.xml
2009-12-14 21:50:21	msnportal.112.2o7.net		[redacted]	info.xml
2009-12-14 21:50:17	c.atdmt.com	c.atdmt.com.nsatc.net	[redacted]	info.xml
2009-12-14 21:50:16	c.live.com	c.live.com.nsatc.net	[redacted]	info.xml
2009-12-14 21:50:16	c.live.com	c.live.com.nsatc.net	[redacted]	info.xml
2009-12-14 21:50:16	c.atdmt.com	c.atdmt.com.nsatc.net		info.xml

Previous 1 | 2 | 3 | 4 | 5 1 of 5 Next

3. **Web site:** Entering in Web menu we can view all HTTP contents of the session. We can select or search a content. Clicking on a link will open a new page (separated), in which, with Xplico System, will rebuild the full URL of that page, contained in pcap decoded. Xplico System simulate the original cache of the browser, of course if the pcap (in all sessions of case) contain the data to simulate the cache. Everything works if and only if the proxy is enabled in Firefox and it is pointing to the server that runs Xplico System.



For a complete view of html page set your browser to use Proxy, and point it to Web server.

Web URLs: ○ Html ○ Image ○ Flash ○ Video ○ Audio ○ JSON ● All

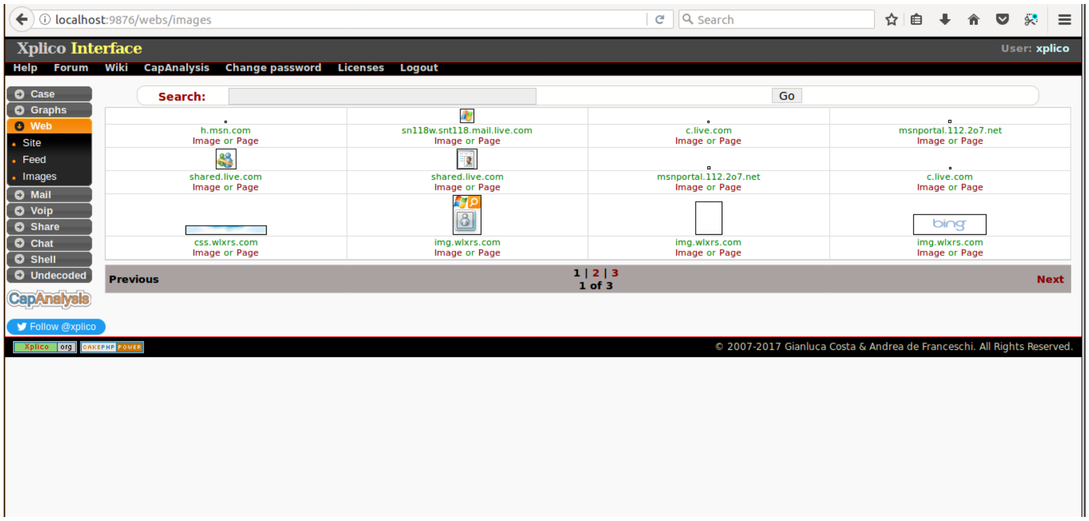
Search: Go

Date	Url	Size	Method	Info
2009-12-14 21:51:00	sn118w.snt118.mail.live.com/im/pages/ToastMini.aspx	1009	GET	info.xml
2009-12-14 21:50:56	sn118w.snt118.mail.live.com/im/pages/BuddyList.aspx	1962	GET	info.xml
2009-12-14 21:50:56	sn118w.snt118.mail.live.com/im/pages/ToastFull.aspx	2213	GET	info.xml
2009-12-14 21:50:51	rad.msn.com/ADSAdClient31.dll?GetSAd=&DPJS=4&PN=MSFT&ID=C9F912A3D2F7D431F8CBA8EDFFFFFFFF&MUID=DEF4FE7FA4D	477	GET	info.xml
2009-12-14 21:50:51	view.atdmt.com/D5I/iview/136566009/direct;wi.160;hi.600/01?click=	4610	GET	info.xml
2009-12-14 21:50:51	a.rad.msn.com/ADSAdClient31.dll?GetSAd=&DPJS=4&PN=MSFT&ID=C9F912A3D2F7D431F8CBA8EDFFFFFFFF&MUID=DEF4FE7FA4	1011	GET	info.xml
2009-12-14 21:50:50	h.msn.com/c.gif?RF=&PI=7324&DI=5707&PS=96690&cb=1260823850606	42	GET	info.xml
2009-12-14 21:50:50	sn118w.snt118.mail.live.com/im/pages/im.aspx	8410	GET	info.xml
2009-12-14 21:50:49	sn118w.snt118.mail.live.com/favicon.ico	1406	GET	info.xml
2009-12-14 21:50:49	sn118w.snt118.mail.live.com/mail/InboxLight.aspx?n=1641341718	16018	GET	info.xml
2009-12-14 21:50:49	sn118w.snt118.mail.live.com/default.aspx?n=424857020	1558	GET	info.xml
2009-12-14 21:50:47	shared.live.com/eRJxj!uCczzilb4hGipZXQ//js/CategoryPicker.js	1264	GET	info.xml
2009-12-14 21:50:47	c.live.com/c.gif?NC=31263&NA=1149&PS=97598&PI=94811&DI=13263&TP=spaces.live.com-&GT1=;	42	GET	info.xml
2009-12-14 21:50:47	msnportal.112.2o7.net/b/ss/msnspacesus/1/H.6-pdv-2/s2517528184171?[AQB]&ndh=1&t=14/11/2009%2021%3A50%3A47%201%2	43	GET	info.xml
2009-12-14 21:50:46	msc.wlxrs.com/3aSgPrbZPOt7yAbi7!U!ZQ/js/hip.js	816	GET	info.xml
2009-12-14 21:50:41	shared.live.com/7E81kqTseEOmzDlpeFPS8g/Web/images/wlmessenger_24x24.gif	400	GET	info.xml

Previous 1 | 2 | 3 | 4 | 5 1 of 5 Next

© 2007-2017 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

4. **Images:** To get an overview of all images transported by HTTP protocol we can access to the menu Images.



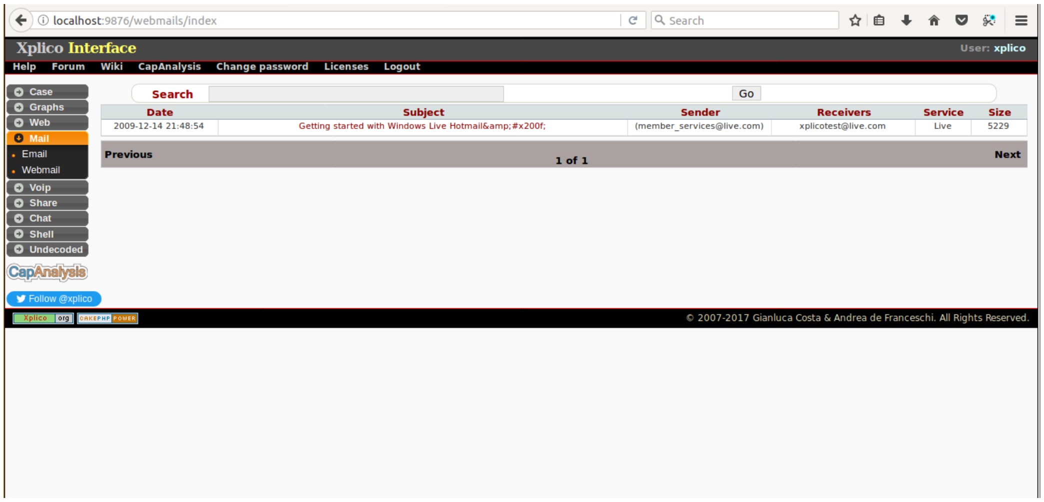
Search: Go

h.msn.com Image or Page	sn118w.snt118.mail.live.com Image or Page	c.live.com Image or Page	msnportal.112.2o7.net Image or Page
shared.live.com Image or Page	shared.live.com Image or Page	msnportal.112.2o7.net Image or Page	c.live.com Image or Page
css.wlxrs.com Image or Page	img.wlxrs.com Image or Page	img.wlxrs.com Image or Page	img.wlxrs.com Image or Page

Previous 1 | 2 | 3 1 of 3 Next

© 2007-2017 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

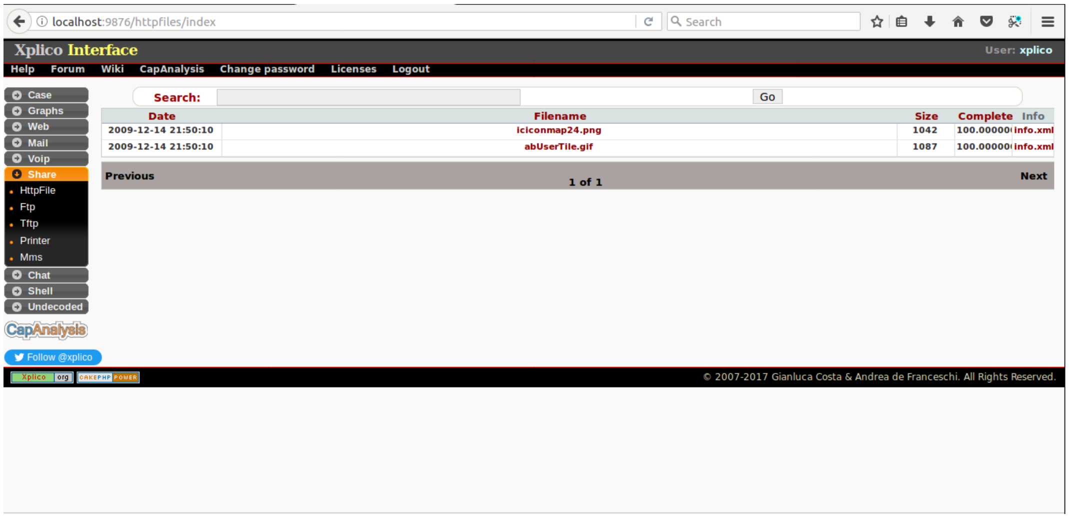
5. **Web Mail:** The search form permits us to find email by subject, receivers, and sender. Selecting one of the emails you see it even if it is in html and contains files attached. For each email we can obtain the PCAP with only the flow that contains it. To do that we have to point the mouse upon the info line and click pcap link.



Date	Subject	Sender	Receivers	Service	Size
2009-12-14 21:48:54	Getting started with Windows Live Hotmail&#x200f;	(member_services@live.com)	xplicotest@live.com	Live	5229

© 2007-2017 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

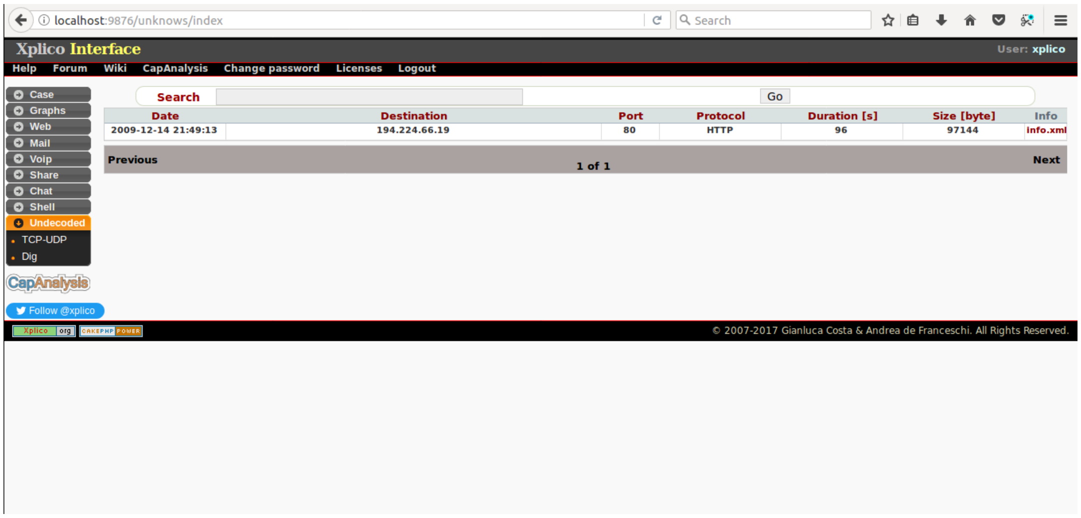
6. **HTTP file share:** It displays time accessed, file name, size of the file shared and pcap file



Date	Filename	Size	Complete	Info
2009-12-14 21:50:10	iciconmap24.png	1042	100.00000	info.xml
2009-12-14 21:50:10	abUserTile.gif	1087	100.00000	info.xml

© 2007-2017 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

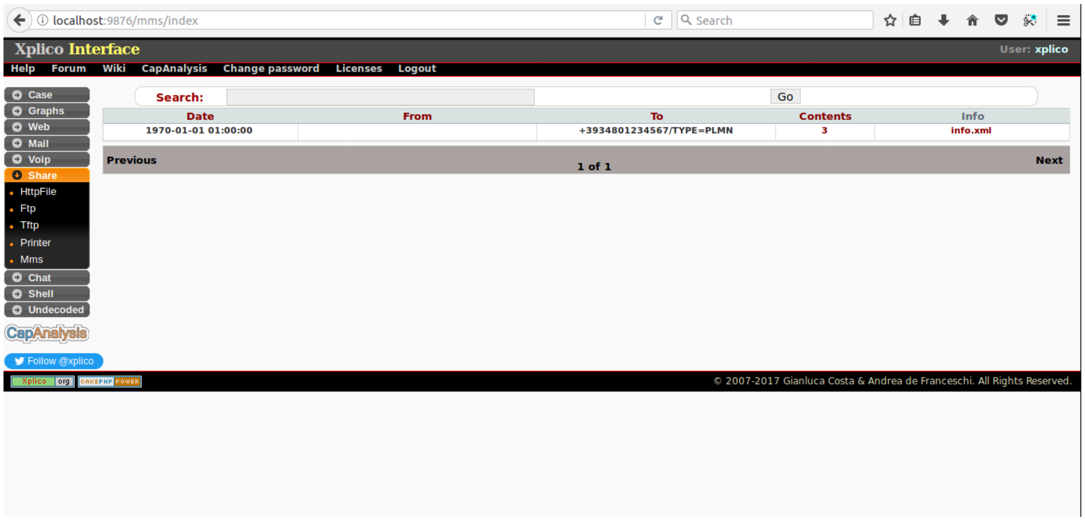
7. **TCP:** TCP stands for Transmission Control Protocol. It displays accesses time, destination, port, protocol, duration, size of the file and pcap file.



Date	Destination	Port	Protocol	Duration [s]	Size [byte]	Info
2009-12-14 21:49:13	194.224.66.19	80	HTTP	96	97144	info.xml

© 2007-2017 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

8. **MMS:** If the MMS messages (Multimedia Messaging Service) are transported by HTTP protocol then Xplico decoder can decompose the MMS message into its content, i.e., text, video, and images. The main page of MMS reports the list of MMS decoded



Date	From	To	Contents	Info
1970-01-01 01:00:00		+3934801234567/TYPE=PLMN	3	info.xml

© 2007-2017 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Questions:

1. What is the information we find in GeoMap?
2. Where can we find the HTTP contents, such as the URL?
3. Where can we find the images that were surfed?
4. What is the information we find in Webmail?
5. What does the info.xml file contain for sessions?