

Lab 12 - Module 12.1: Remote acquisition with Xplico

Objectives

- To perform packet sniffing to generate a pcap file
- Use Xplico to examine the pcap files generated
- Use Xplico to perform live acquisition on the investigation machine

Task 1: Generate two pcap files

Step 1: Perform a task on machine-1 to generate a pcap file

1. Open Windows Command Prompt as an administrator on machine 1
2. Use below command to list available interfaces
pktmon comp list
3. Use the below command to start the packet capture. By default, the pcap file will be generated a file named PktMon.etl in the current working directory.

pktmon start --etw -c <interface_id>

If no interface_id there, then just enter the command *pktmon start --etw -c*

4. **Perform a task on machine 1.**

For example, download nginx from the link: <http://nginx.org/en/download.html>

Manage NGINX instances with NGINX Agent, an open source daemon providing observability data and remote configuration
[Learn more](#)

nginx: download

Mainline version


CHANGES	nginx-1.23.3 pgp	nginx/Windows-1.23.3 pgp
-------------------------	--	--

Stable version

CHANGES-1.22	nginx-1.22.1 pgp	nginx/Windows-1.22.1 pgp
------------------------------	--	--

Legacy versions

CHANGES-1.20	nginx-1.20.2 pgp	nginx/Windows-1.20.2 pgp
CHANGES-1.18	nginx-1.18.0 pgp	nginx/Windows-1.18.0 pgp
CHANGES-1.16	nginx-1.16.1 pgp	nginx/Windows-1.16.1 pgp
CHANGES-1.14	nginx-1.14.2 pgp	nginx/Windows-1.14.2 pgp
CHANGES-1.12	nginx-1.12.2 pgp	nginx/Windows-1.12.2 pgp
CHANGES-1.10	nginx-1.10.3 pgp	nginx/Windows-1.10.3 pgp
CHANGES-1.8	nginx-1.8.1 pgp	nginx/Windows-1.8.1 pgp
CHANGES-1.6	nginx-1.6.3 pgp	nginx/Windows-1.6.3 pgp



- [english](#)
- [русский](#)
- [news](#)
- [about](#)
- [download](#)
- [security](#)
- [documentation](#)
- [faq](#)
- [books](#)
- [support](#)
- [trac](#)
- [twitter](#)
- [blog](#)
- [unit](#)
- [djs](#)

6. After you performed the task needed, stop the packet capture using below command
pktmon stop
7. Convert the .etl file to the Xplico supported pcap format using below command.
For example: *pktmon pcap PktMon.etl -o taskperformed.pcap*
pktmon <format> <source_path> -o <source_output>

Step 2: Do not perform a task on machine-2 and generate a pcap file

1. Open Windows Command Prompt as an administrator on machine 2
2. Use below command to list available interfaces
pktmon comp list
3. Use the interface Id from the pktmon comp list output to start the packet capture before performing the task scan or task that the packet capture is needed for. By default, the pcap file will be generated a file named PktMon.etl in the current working directory.
pktmon start --etw -c <interface_id>
If no interface_id there, then just enter the command *pktmon start --etw -c*
4. **Do not perform a task on machine-2.** Just simply scan the idle machine 2
5. Stop the packet capture using below command
pktmon stop
6. Convert the ETL to the WireShark supported pcap format with the below command.
For example: *pktmon pcap PktMon.etl -o notaskperformed.pcap*
pktmon <format> <source_path> -o <source_output>

Task 2: Install Xplico and login

In this module, we use ubuntu 64-bit operating system machine-3 as an investigation machine (For example the Kali Linux machine).

1. Open terminal as run as administrator and locate to root folder

```
sudo -i
(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
└─(root㉿kali)-[~]
#
```

2. Run below commands to install Xplico

apt install xplico

And then enter “y” to continue installing Xplico.

```
(root㉿kali)-[~]
# apt install xplico
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binfmt-support lame libndpi4.2 libopencore-amrnb0 libopencore-amrwb0
  librecode0 libsox-fmt-alsa libsox-fmt-base libsox3 php-sqlite3
  php8.2-sqlite3 python3-httpplib2 recode sox
Suggested packages:
  lame-doc libsox-fmt-all
The following NEW packages will be installed:
  binfmt-support lame libndpi4.2 libopencore-amrnb0 libopencore-amrwb0
  librecode0 libsox-fmt-alsa libsox-fmt-base libsox3 php-sqlite3
  php8.2-sqlite3 python3-httpplib2 recode sox xplico
0 upgraded, 15 newly installed, 0 to remove and 258 not upgraded.
Need to get 4,139 kB of archives.
After this operation, 17.4 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
root@kali: ~  
File Actions Edit View Help  
Creating config file /etc/php/8.2/mods-available/sqlite3.ini with new version  
Creating config file /etc/php/8.2/mods-available/pdo_sqlite.ini with new version  
Setting up php-sqlite3 (2:8.2+93) ...  
Setting up sox (14.4.2+git20190427-3.5) ...  
Setting up xplico (1.2.2-0kali6) ...  
Enabling module rewrite.  
To activate the new configuration, you need to run:  
    systemctl restart apache2  
Module mpm_event already disabled  
Considering conflict mpm_event for mpm_prefork:  
Considering conflict mpm_worker for mpm_prefork:  
Module mpm_prefork already enabled  
update-rc.d: We have no instructions for the xplico init script.  
update-rc.d: It looks like a network service, we disable it.  
xplico.service is a disabled or a static unit, not starting it.  
Processing triggers for mailcap (3.70+nmu1) ...  
Processing triggers for kali-menu (2023.2.3) ...  
Processing triggers for libc-bin (2.36-9) ...  
Processing triggers for man-db (2.11.2-2) ...  
Processing triggers for libapache2-mod-php8.2 (8.2.5-2) ...  
Processing triggers for php8.2-cli (8.2.5-2) ...  
  
(root@kali)-[~]  
#
```

Installation finished.

3. After successful installation. We must restart Apache2 using below commands

service apache2 restart

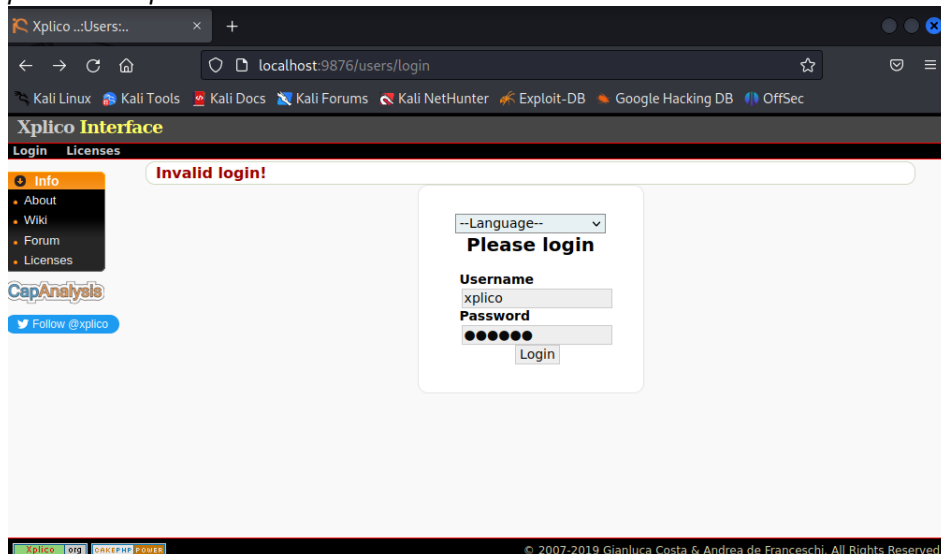
service xplico start

```
(root@kali)-[~]  
# service apache2 start  
  
(root@kali)-[~]  
# service xplico start  
  
(root@kali)-[~]  
#
```

4. Minimize the terminal and let it keeps running in the background. Do not close the terminal.
5. Next, open url <http://localhost:9876> (Xplico Interface login) in browser
6. Login into Xplico using below credentials

username: xplico

password: xplico

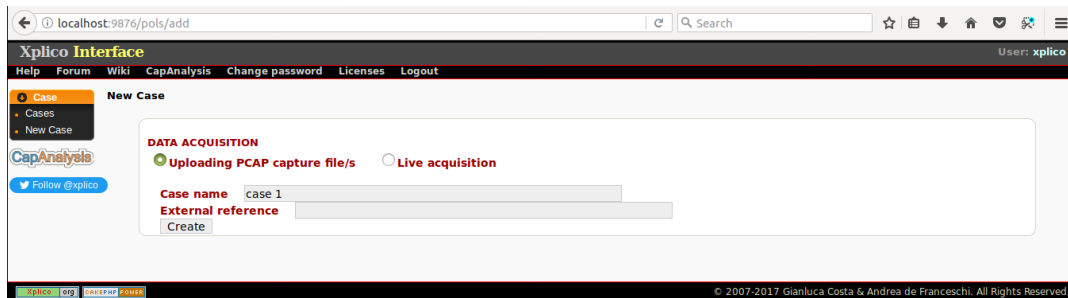


Packet Sniffing

Task 3: Analyze machine-1 and machine-2 pcap files

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 1' and click on create



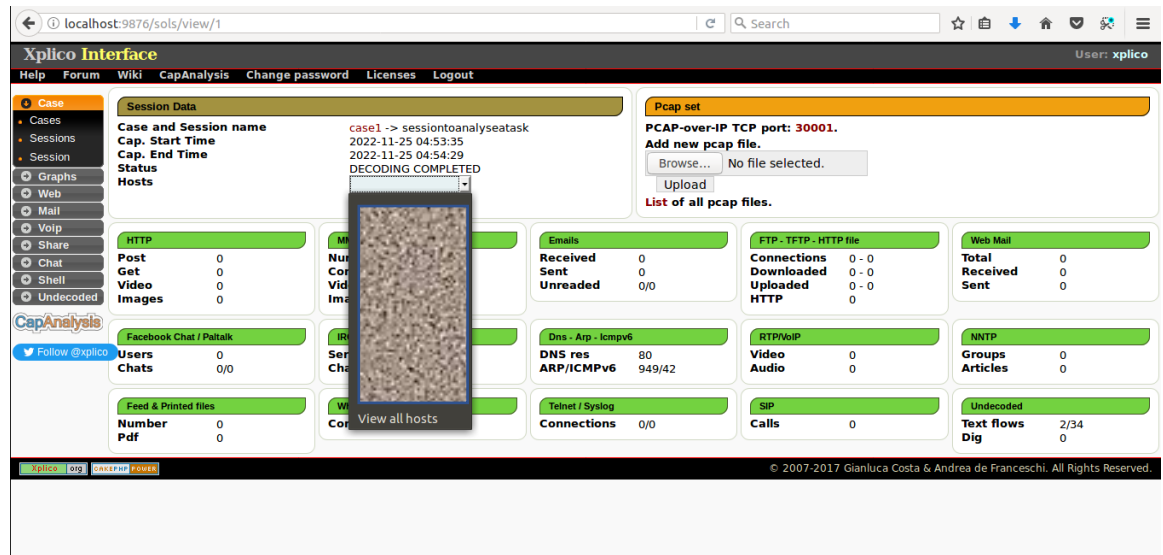
3. New case is successfully created
4. Click on Case 1

Step 2: Create a session

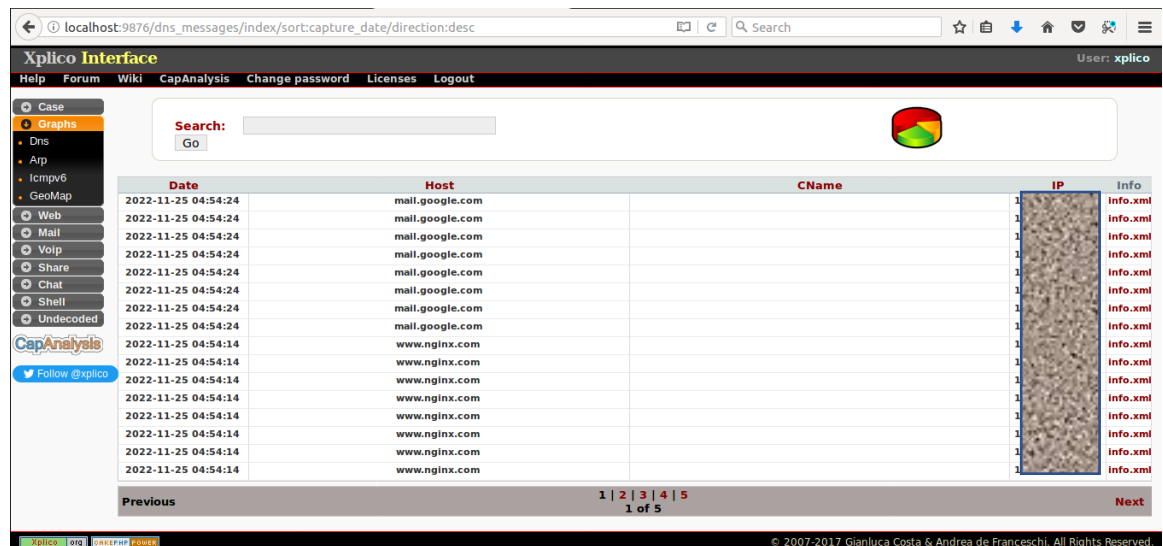
1. In case 1, click on new session
2. Provide session name as 'session to analyse a task'

Step 3: Analyze machine-1 pcap file

1. In 'session to analyse a task' session, click browse
2. Select the machine-1 pcap file we generated in task #1 step #1. For example: taskperformed.pcap
3. Click upload and wait until the file is decoded
4. Next, after successful decoding, click hosts dropdown and select 'view all hosts' and click filter



5. Now start analyzing the data. You can check as below:
 - a) Go to graphs and click Dns. Here you can find the website nginx on hosts from where we downloaded the software as a task



- b) Go to undecoded and click on TCP. Here you can find Date, port, size, duration of the task performed we performed in task #1 step #1

Date	Destination	Port	Protocol	Duration [s]	Size [byte]	Info
2022-11-25 04:54:25	10.0.0.1	5	Unknown	0	711	info.xml
2022-11-25 04:54:24	10.0.0.1	5	Unknown	1	7565	info.xml
2022-11-25 04:54:23	10.0.0.1	5	Unknown	0	2292	info.xml
2022-11-25 04:54:20	10.0.0.1	5	Unknown	0	711	info.xml
2022-11-25 04:54:16	10.0.0.1	5	Unknown	10	12500	info.xml
2022-11-25 04:54:15	10.0.0.1	5	Unknown	0	711	info.xml
2022-11-25 04:54:13	10.0.0.1	5	Unknown	15	78	info.xml
2022-11-25 04:54:11	10.0.0.1	5	Unknown	0	7250	info.xml
2022-11-25 04:54:10	10.0.0.1	5	Unknown	0	711	info.xml
2022-11-25 04:54:06	10.0.0.1	5	Unknown	1	2944	info.xml
2022-11-25 04:54:05	10.0.0.1	5	Unknown	0	711	info.xml
2022-11-25 04:54:01	10.0.0.1	5	Unknown	0	3400	info.xml
2022-11-25 04:54:01	10.0.0.1	5	Unknown	0	7369	info.xml
2022-11-25 04:54:00	10.0.0.1	5	Unknown	0	711	info.xml
2022-11-25 04:53:55	10.0.0.1	5	Unknown	0	711	info.xml
2022-11-25 04:53:52	10.0.0.1	5	Unknown	0	1976	info.xml

Step 4: Create a session

1. In case 1, click on new session
2. Provide session name as 'session to analyse a no task'

Step 5: Analyze machine-2 pcap file

1. In 'session to analyse a no task' session, click browse
2. Select the machine-2 pcap file we generated in task #1 step #2
3. Click upload and wait until the file is decoded
4. Next, after successful decoding, click on hosts dropdown and select 'view all hosts' and click on filter
5. Now start analyzing the data. You can check as below:
 - a) Go to graphs and click Dns. Here you can find no hosts as we did not perform any task on machine 2

Date	Host	CName	IP	Info
Previous				
1 of 1				
Next				

- b) Go to undecoded and click on TCP. Here you can find Date, port, size, duration

Date	Destination	Port	Protocol	Duration [s]	Size [byte]	Info
2022-11-25 08:04:50		5	Unknown	0	711	info.xml
2022-11-25 08:04:45		5	Unknown	0	711	info.xml
2022-11-25 08:04:43		2	Unknown	7	408	info.xml
2022-11-25 08:04:42		4	Unknown	9	178164	info.xml
2022-11-25 08:04:42		5	Unknown	9	39168	info.xml

Live Acquisition

Task 4: Live acquisition on machine 3

Step 1: Initiate the live acquisition

1. On Xplico interface, go to cases and click on 'new cases'
2. Select 'live acquisition' and provide case name as 'case 2'

New Case

DATA ACQUISITION

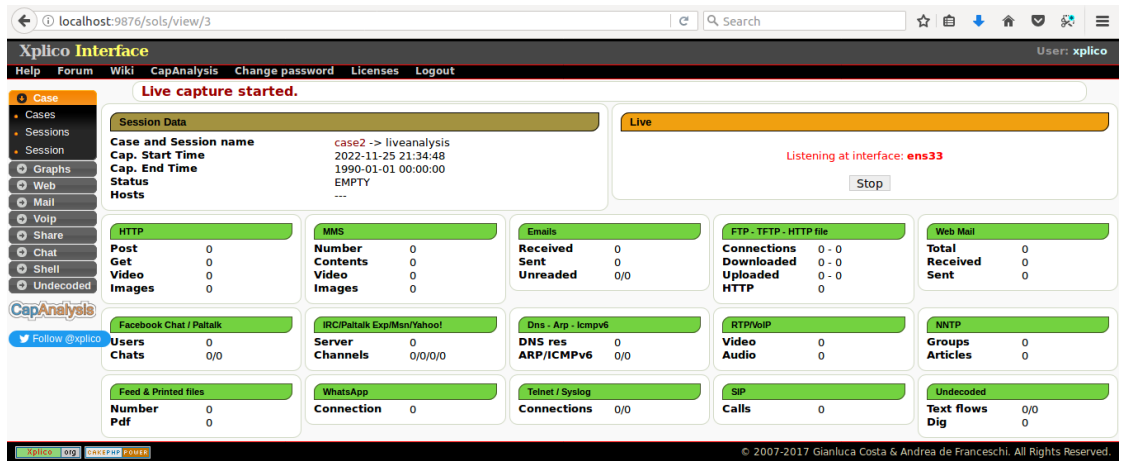
☐ Uploading PCAP capture file/s ☒ Live acquisition

Case name: case 2

External reference:

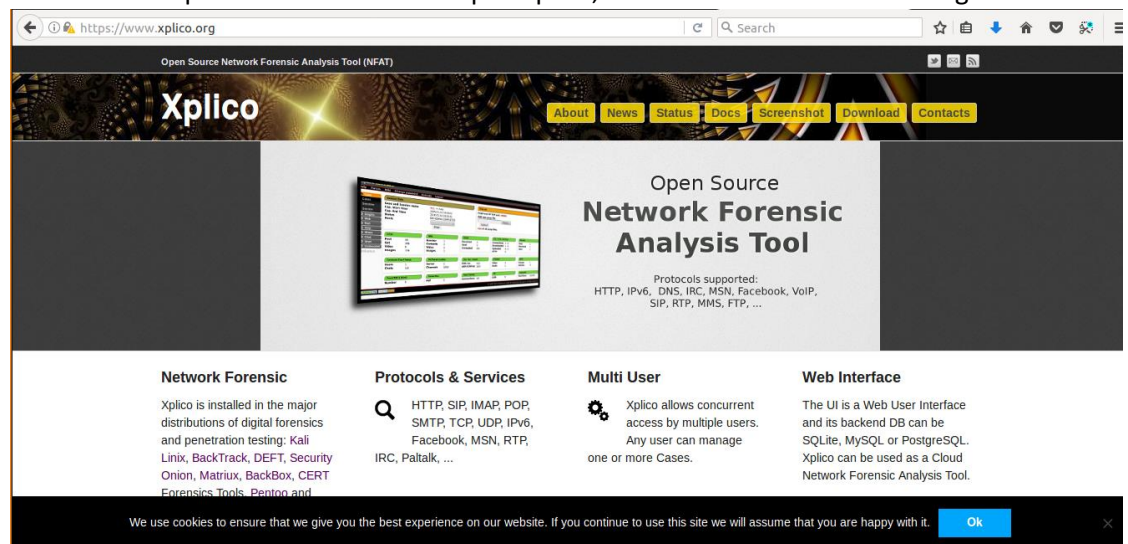
Create

3. Click on create and Case 2 is successfully created
4. Click on case 2 and go to new session and provide name as 'session for live acquisition' and click on create
5. Next, click on interface and select the interface and click on start
6. Next, in the session created, click on hosts dropdown, and select 'view all hosts' and click on filter
7. The live acquisition is started



Step 2: Analyse the acquisition

1. On machine-3 perform few tasks like open xplico, or a website and start tracking them



2. Start analyzing the data
 - a) Go to graphs and click Dns. Here you can find the live data websites on hosts

localhost:9876/dns_messages/index/sort:capture_date/direction:desc

Xplico Interface User: xplico

Help Forum Wiki CapAnalysis Change password Licenses Logout

Search: Go

Date	Host	CName	IP	Info
2022-11-25 22:36:59	syndication.twitter.com			Info.xml
2022-11-25 22:36:59	www.capanalysis.net			Info.xml
2022-11-25 22:36:59	wiki.xplico.org			Info.xml
2022-11-25 22:36:59	forum.xplico.org			Info.xml
2022-11-25 22:36:59	twitter.com			Info.xml
2022-11-25 22:36:59	www.xplico.org			Info.xml
2022-11-25 22:36:59	www.cakephp.org			Info.xml
2022-11-25 22:36:59	www.cakephp.org			Info.xml
2022-11-25 22:36:58	platform.twitter.com	cs472.wac.edgecastcdn.net		Info.xml
2022-11-25 22:36:58	platform.twitter.com	cs472.wac.edgecastcdn.net		Info.xml
2022-11-25 22:36:47	chat-dl.google.com			Info.xml
2022-11-25 22:36:47	chat-dl.google.com			Info.xml
2022-11-25 22:36:32	chat-dl.google.com			Info.xml
2022-11-25 22:36:32	chat-dl.google.com			Info.xml
2022-11-25 22:36:26	signaler-pa.clients6.google.com			Info.xml
2022-11-25 22:36:26	signaler-pa.clients6.google.com			Info.xml

Previous 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 1 of 16 Next

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

- b) Go to undecoded and click on TCP. Here you can find Date, port, size, duration of the live tasks performed
3. Go to session and click Stop to stop the acquisition

localhost:9876/sols/view/3

Xplico Interface User: xplico

Help Forum Wiki CapAnalysis Change password Licenses Logout

Live capture stopped.

Session Data

Case and Session name case2 -> liveanalysis

Cap. Start Time 2022-11-25 21:34:48

Cap. End Time 2022-11-25 21:37:43

Status DECODING

Filter

Interface: Start

HTTP	MMS	Emails	FTP - TFTP - HTTP file	Web Mail
Post 0	Number 0	Received 0	Connections 0 - 0	Total 0
Get 0	Contents 0	Sent 0	Downloaded 0 - 0	Received 0
Video 0	Video 0	Unreaded 0/0	Uploaded 0 - 0	Sent 0
Images 0	Images 0		HTTP 0	

Facebook Chat / Paltalk	IRC/Paltalk Exp/Non/Yahoo!	Dns - Arp - Icmpv6	RTP/MiP	NNTP
Users 0	Server 0	DNS res 264	Video 0	Groups 0
Chats 0/0	Channels 0/0/0/0	ARP/ICMPv6 36/0	Audio 0	Articles 0

Feed & Printed files	WhatsApp	Telnet / Syslog	SIP	Undecoded
Number 0	Connection 0	Connections 0/0	Calls 0	Text flows 0/18
Pdf 0				Dig 0

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

Questions:

1. What is the command we used to start the packet capture?
2. What is the command we used to convert the generated ETL to a pcap format?
3. What is the purpose of converting an ETL file to a pcap file?
4. What are the two different data acquisition techniques we used in this module?
5. What is the command to start the Xplico decoding manager?