

[Contact](#)
[Affiliate](#)
[Blackploit](#)
[Sumit a Tool](#)

[Home](#)
[Windows](#)
[GNU/Linux](#)
[OS X](#)
[Android](#)
[iPhone](#)
[Categories ▾](#)

**16周年 特別記念**  
**年 キャンペーン**

**.com .net ドメイン 580円から**  
**この価格は期間限定!**

Labels ▾

Search

Subscribe via e-mail



Subscribe via e-mail

Subscribe

**Python for Offensive Penetration Testing**  
 Learn how to hack using Python  
 One Time Offer **15\$**

Run a website scan for SQLi, XSS  
and other vulnerabilities with



Home » Forensic Analyzer » Linux » Network Forensic Analysis Tool » NFAT » Xplico » Xplico v1.1.1 - Open Source Network Forensic Analysis Tool (NFAT)

## Xplico v1.1.1 - Open Source Network Forensic Analysis Tool (NFAT)

Lydecker Black on 5:54 PM

**Xplico Interface**
User: deft

[Help](#)
[Logout](#)

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 ☐ All

Cases	Sols	Date	Url	Size	Method	Info
		2007-08-14 11:13:58	www.google.it/	1521	GET	info.xml
		2007-08-14 11:13:33	track3.mybloglog.com/tr/urtrk.php?i=2007011710424247&t=1&u=http://33a/www.aphotoe	105	GET	info.xml
		2007-08-14 11:13:32	track3.mybloglog.com/js/jserv.php?mbid=2007011710424247	5276	GET	info.xml
		2007-08-14 11:13:25	track3.mybloglog.com/tr/urtrk.php?i=2007011710424247&t=1&u=http://33a/www.aphotoe	105	GET	info.xml
		2007-08-14 11:13:24	track3.mybloglog.com/js/jserv.php?mbid=2007011710424247	5274	GET	info.xml
		2007-08-14 11:13:23	rcm.amazon.com/cm?i=ap06-20&e=1&p=20&l=qs1&f=ifr	2669	GET	info.xml
		2007-08-14 11:13:10	rcm.amazon.com/cm?i=ap06-20&e=1&p=20&l=qs1&f=ifr	2669	GET	info.xml
		2007-08-14 11:13:04	www.aphotoday.org/fronts.html	850	GET	info.xml
		2007-08-14 11:12:37	www.aphotoday.org/apadnews/	3793	GET	info.xml
		2007-08-14 11:12:26	c14.statcounter.com/text.php?sc_project=1435373&resolution=1280&camefrom=http://33a	25	GET	info.xml
		2007-08-14 11:12:23	www.aphotoday.org/favicon.ico	320	GET	info.xml
		2007-08-14 11:12:08	www.aphotoday.org/favicon.ico	320	GET	info.xml
		2007-08-14 11:12:08	www.aladingenius.com/theMagicLamp/	6775	GET	info.xml
		2007-08-14 11:12:07	www.aphotoday.org/bestof2006/	604	GET	info.xml
		2007-08-14 11:12:07	www.aphotoday.org/	1390	GET	info.xml
		2007-08-14 11:12:02	www.photoblogdirectory.org/buttons/photoblogdirectory_bv.gif	1606	GET	info.xml
		2007-08-14 11:11:52	www.aladingenius.com/templates/themagiclamp_2006/img/back.gif	238	GET	info.xml
		2007-08-14 11:11:51	www.aladingenius.com/theMagicLamp/index.php?x=browse&pagenum=1	14029	GET	info.xml
		2007-08-14 11:11:47	www.aladingenius.com/templates/themagiclamp_2006/img/back.gif	238	GET	info.xml
		2007-08-14 11:11:42	www.aladingenius.com/favicon.ico	209	GET	info.xml

The goal of Xplico is extract from an internet traffic capture the applications data contained.

For example, from a pcap file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP), FTP, TFTP, and so on. Xplico isn't a network protocol analyzer. Xplico is an open source Network Forensic Analysis Tool (NFAT).

Easy, Automated and Scalable  
Web Application Security



Register For a Free Trial

### Features

- Protocols supported: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6, ...;
- Port Independent Protocol Identification (PIPI) for each application protocol;
- Multithreading;
- Output data and information in SQLite database or Mysql database and/or files;
- At each data reassembled by Xplico is associated a XML file that uniquely identifies the flows and the pcap containing the data reassembled;
- Realtime elaboration (depends on the number of flows, the types of protocols and by the performance of computer -RAM, CPU, HD access time, ...-);
- TCP reassembly with ACK verification for any packet or soft ACK verification;
- Reverse DNS lookup from DNS packages contained in the inputs files (pcap), not from external DNS server;
- No size limit on data entry or the number of files entrance (the only limit is HD size);
- IPv4 and IPv6 support;
- Modularity. Each Xplico component is modular. The input interface, the protocol decoder



Submit a Tool



Do Your 2015 IT Plans Include  
Server Migrations?

Explore Your Options With Our Near-Zero Downtime  
Migration Guide

Download the FREE Guide »

Follow us!

(Dissector) and the output interface (dispatcher) are all modules;

- The ability to easily create any kind of dispatcher with which to organize the data extracted in the most appropriate and useful to you;

## Download Xplico

Is your website vulnerable to **SQL INJECTION** and **XSS Vulnerabilities**?

**netsparker**  
Web Application Security Scanner

**DOWNLOAD NOW**

Subscribe via e-mail for updates!

Subscribe



103



5



0



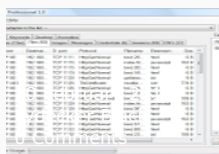
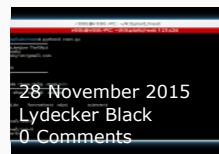
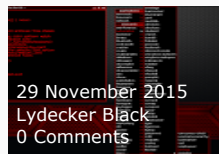
### Next

This is the most recent post.

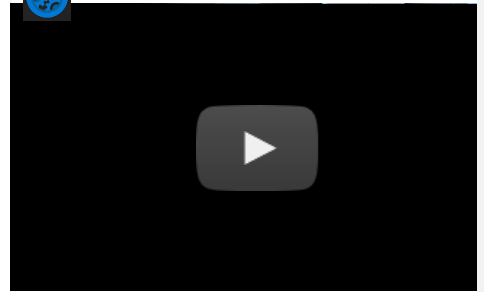
### Previous

[Wordbrutepress - Wordpress Brute Force Multithreading with Standard and XML-RPC Login Method](#)

## Related Posts



Microsoft Mechanics



### Using Server Containers

Wanting to know the advantages of using Containers. Watch Now.



PenTest Tools

Liked

13k likes



Follow @KitPloit

51.2K followers



KitPloit

Follow

+1

+ 4,476

1174 via feed  
BY FEEDBURNER

### Populars

### Comments

### Archive



### REXT - Router Exploitation Toolkit

Small toolkit for easy creation and usage of various python scripts that work with embedded devices. core - contains most of toolkits...



### Sniffly - Sniffing Browser History Using HSTS + CSP.

Sniffly is an attack that abuses HTTP Strict Transport Security and Content Security Policy to allow arbitrary websites to sniff a user&...



### BlackArch Linux v2015.11.24 - Penetration Testing Distribution

BlackArch Linux is an Arch Linux-based distribution for penetration testers and security researchers. The repository...



### Bohatei - Flexible and Elastic DDoS Defense

Bohatei is a first of its kind platform that enables flexible and elastic DDoS defense using SDN and NFV.



### UserProfilesView - View User Profiles Information On Your Windows

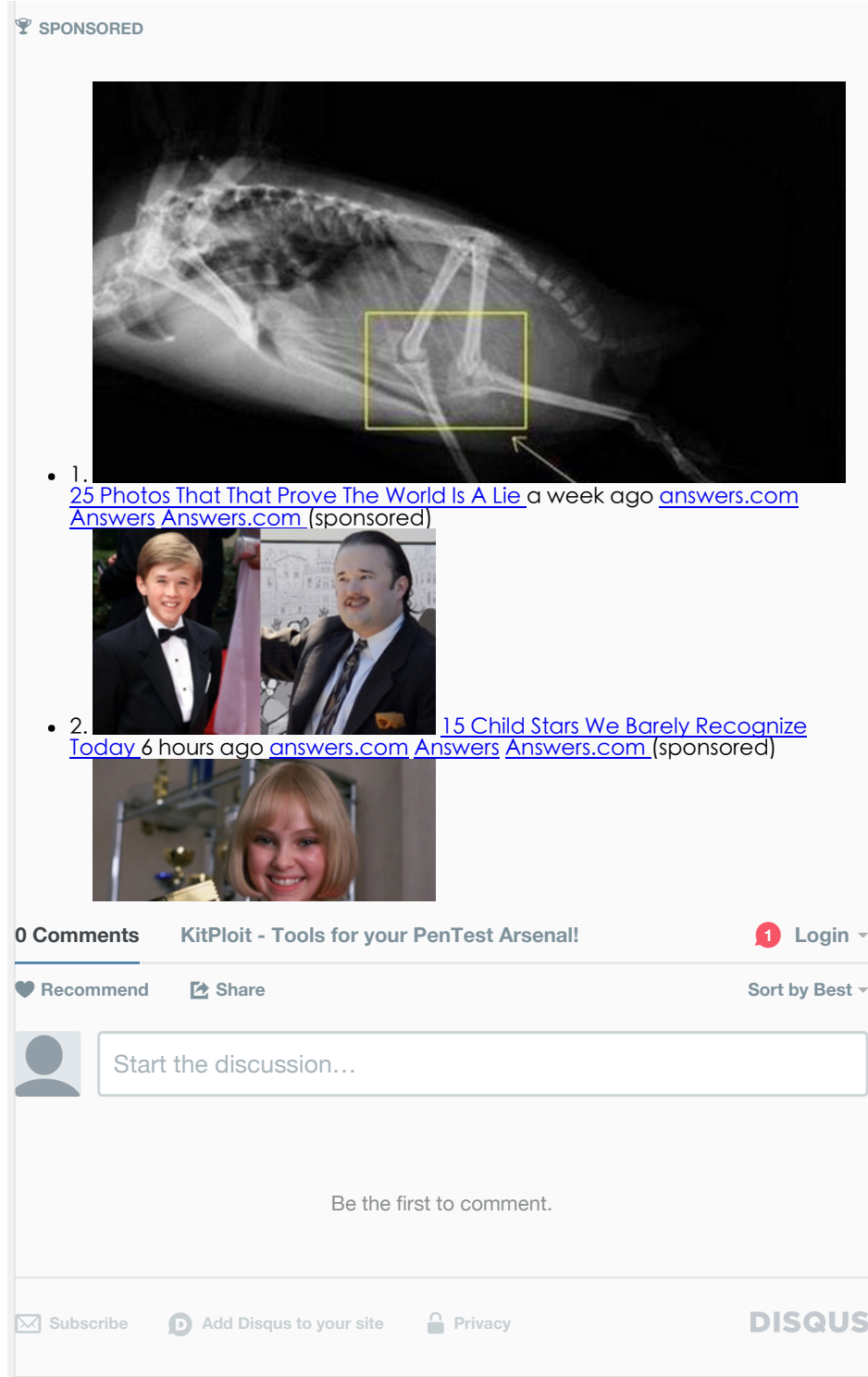
UserProfilesView displays the list of all user profiles that you currently have in your system. For each user profile, the following inf...




### Wordbrutepress - Wordpress Brute Force Multithreading with Standard and XML-RPC Login Method

Wordpress Brute Force Multithreading with standard and xml-rpc login method written in python.


**Xplico v1.1.1 - Open Source Network Forensic Analysis Tool (NFAT)**

SPONSORED




1.

[25 Photos That Prove The World Is A Lie](#) a week ago [answers.com](#)  
[Answers](#) [Answers.com](#) (sponsored)



2.

[15 Child Stars We Barely Recognize Today](#) 6 hours ago [answers.com](#) [Answers](#) [Answers.com](#) (sponsored)



0 Comments


KitPloit - Tools for your PenTest Arsenal!

1 Login

Recommend

Share

Sort by Best



Start the discussion...


Be the first to comment.

Subscribe

Add Disqus to your site

Privacy

DISQUS



The goal of Xplico is extract from an internet traffic capture the applications data contained. For example, from a pcap file Xplic...

Labels

LinuxWindowsMac


ScannerAndroidWireless

Malware AnalysisMalware

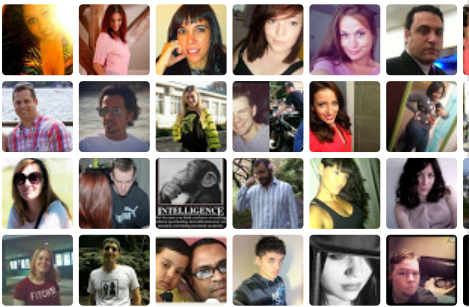
SQLiFacebookiPhone

Cheat SheetKeyloggerRAT

Google+ Followers


KitPloit


Follow




3,584 have us in circles

Fund this site and millions more with Contributor.

Contributor by Google

PenTest Tools

13,403 likes


KitPloit

THE HACKER'S TOOL

Liked

Share

You like this



<b>Site Info</b> kitploit.com Dec 01, 2015	<b>Traffic Rank:</b> 313,590	<b>Links in:</b> 50	Powered by 
--	---------------------------------	------------------------	--

Tweet to @KitPloit

1174 listeners