Xplico

Internet Traffic Decoder. Network Forensic Analysis Tool (NFAT)

By Russ McRee – ISSA member, Puget Sound (Seattle), USA Chapter

Prerequisites

Linux platform – installation methodology described is specific to Ubuntu

When last we discussed a Network Forensic Analysis Tool (NFAT) it was in July 2010's NetWitness Investigator review[1] and August 2008's NetworkMiner[2] write-up. Similarly, Xplico is a project released under GPL that decodes packet captures (PCAP), extracting the likes of email content (POP, IMAP, and SMTP protocols), all HTTP content, VoIP calls (SIP), IM chats, FTP, TFTP, and many others. Check out the Xplico status page[3] for the current state of available protocol dissectors.

In an email exchange with project lead Gianluca Costa (ciao from Venezia!), I learned quite a bit about Xplico. Gianluca and partner Andrea De Franceschi started the Xplico project in 2007 as there were no free tools that reconstructed application network data. They decided to close the gap by designing and developing Xplico as a system (framework) as well as a decoder which could be used without the need to purchase very expensive tools. Xplico can be used on platforms with an embedded ARM core processor or typical multi-core servers, making optimal use of available resources.

1 http://holisticinfosec.org/toolsmith/docs/july2010.html.
2 http://holisticinfosec.org/toolsmith/docs/august2008.pdf.
3 http://www.xplico.org/status.

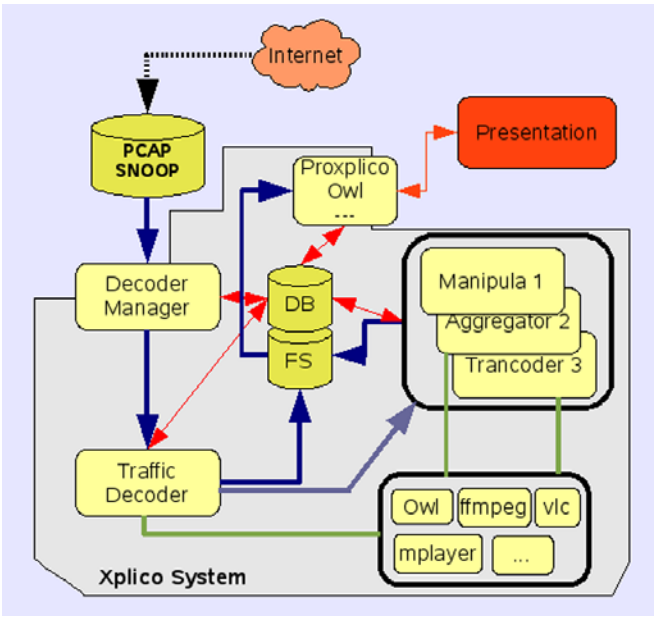


Figure 1 – The Xplico system

Xplico, as a framework, is made up of various components and applications (increasing in number). See Figure 1.

At the core of Xplico is the decoder, accentuated by various manipulators. Xplico has been designed so that you can use the decoder (and manipulators) as stand-alone entities if you wish without necessarily depending on DeMa (decoder manager) or Xplico Web GUI. This allows you the potential use of different database architecture and other GUI options. The architecture promotes a high degree of integration in support of the free and open source model.

With regard to the modular design of the decoder, Xplico provides a broad array of functionality including capture (data acquisition), dissector (protocol decoders), and dispatcher (interface to storage) modules. Need to ensure that your modules conform to the specifications and guidelines of CALEA[4] Lawful Intercept standards or NIST Computer Forensics Tool Testing (CFTT)[5] methodology? No problem; Xplico is designed to support your cause, and the dispatcher logic will make querying the likes of SQLite, MySQL, and flat files supportive of reporting.

The project team is currently finishing the development of:

- Web MSN dissector and manipulator
- VoIP MGCP dissector
- SMB dissector
- Web Yahoo! chat dissector and manipulator
- Improvements to the Python3 script

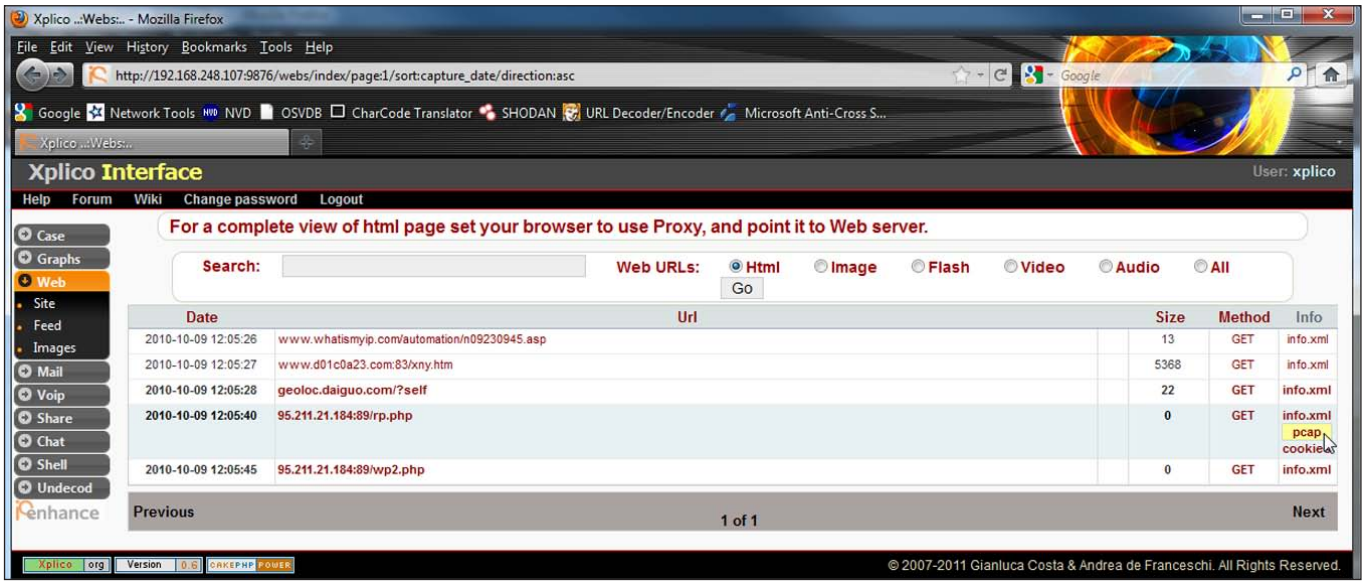
In future months their goals are:

- New WebMail decoder
- ICQ basic dissector
- JABBER basic dissector
- YAHOO chat basic dissector

Count on the inevitable "professional version" as well, including a different Web GUI with new features, and the hopes of economic support for development efforts.

4 http://lawfulintercept.org.
5 http://www.cftt.nist.gov

Figure 2 – Xplico web session decoding



Xplico has been included in BackTrack, DEFT Linux, Orion, GnackTrack, Security Onion, and other similar Live CD/DVD distributions.

The project leads also pointed out that Xplico is discussed under further reading as part of the European project INDECT.[6] Specifically, a paper is cited, "European FP7-SEC: On detecting Internet-based criminal threats with XplicoAlerts," wherein the authors developed an extension of Xplico called XplicoAlerts (remember that extensible modularity already mentioned?). This paper[7] is a worthy read if for no other reason than to illuminate Xplico's strong suits.

Installation

I focused my installation efforts on the latest version of Ubuntu (11.04) as I found that dependencies for Xplico 0.6.2 were not easily met on earlier versions. Working with version 0.6.2 was important to me as it includes layer seven pattern classifiers (application) for "all flows not decoded" along with other improvements.

On Ububtu 11.04 (Natty Narwhal) the following script executed at a terminal prompt will ensure a one-step installation, including a download of the .deb package (ripped and modified from a tal.ki forum[8]):

```
sudo apt-get update && sudo apt-get
install -y gdebi sed && wget http://
sourceforge.net/projects/xplico/files/
Xplico%20versions/version%200.6.2/
xplico_0.6.2_i386.deb && sudo gdebi -n
xplico* && sudo find /etc/php5/apache2/
php.ini -exec sed -i.bak 's/post_max_
size = 8M/post_max_size = 800M/g; s/
upload_max_filesize = 2M/upload_max_
filesize = 400M/g' {} \; && sudo service
apache2 restart && sudo service xplico
restart && firefox localhost:9876
```

If you wish to roll Xplico from source or work through your own installation options with the Debian/Ubuntu package, grab the bits from SourceForge.[9]

Analyzing PCAPs with Xplico

Login to Xplico via a browser on your local host or from a remote system with access to the Xplico server; the session will be bound to port 9876 by default: `http://<XplicoHost>:9876`. The default username and password are (you guessed it) xplico/xplico. If you wish to make use of administrative functionality such as changing the default password ;-) log in as *admin/xplico*.

Begin by clicking *New Case* and name your case appropriately; I utilized *toolsmith* for this exercise.

Click the new case in the *Cases List* and choose *New Session*. I recommend choosing names for your sessions that are specific to the PCAPs you're going to analyze. Perhaps yours is a more forensic effort and there are applicable case (evidence) numbers for PCAPs, or you're utilizing Xplico for network analysis specific to malware behavior.

Click the new session from *List of listening sessions*, then upload your intended PCAP. Note that you can choose to acquire a capture from a listening interface on the Xplico host in addition to uploading already acquired network captures.

The first capture I uploaded was one taken from a Renocide/Harakit worm runtime analysis.

Renocide is a pervasive, annoying little b#$%^&d; if you've had to hunt it down and kill it, you know exactly what I mean.

You'll receive a "File uploaded, wait start decoding..." message while the uploaded PCAP is decoded by Xplico.

The results from this particular capture weren't all that extraordinary, but Xplico capably grabbed all the web requests this Renocide variant made when it phoned home for more

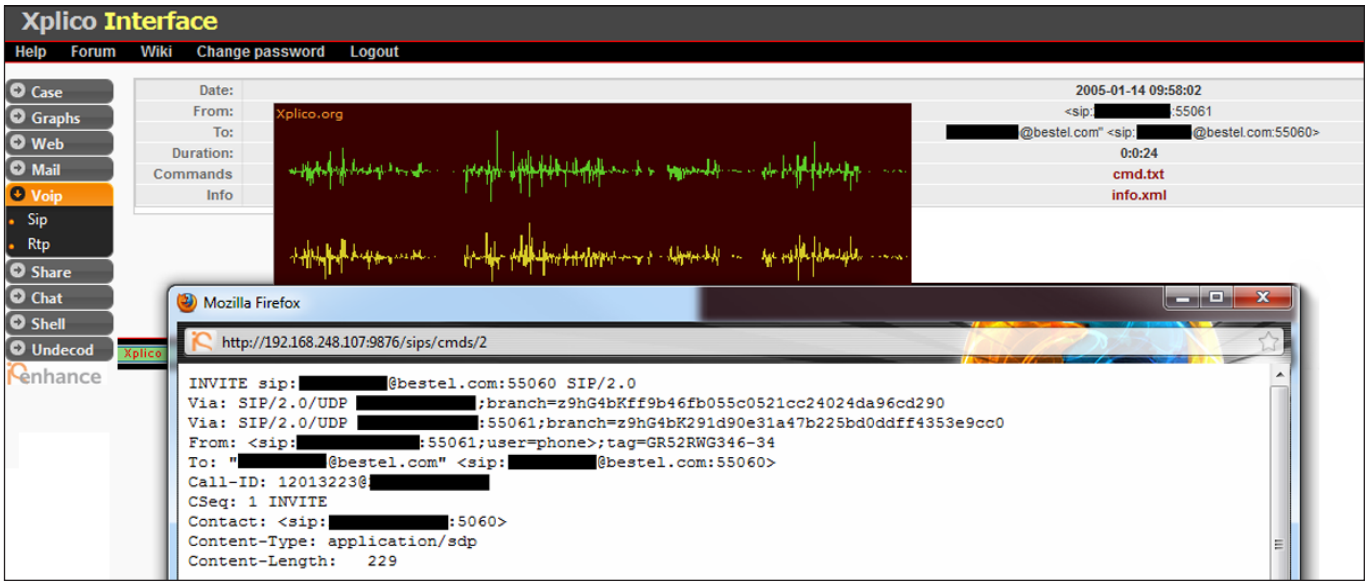
6 http://en.wikipedia.org/wiki/INDECT.

7 http://www.it.uc3m.es/~muruenya/papers/MCSS10XplicoAlerts.pdf.

8 http://5ff1cwepqm.tal.ki/20101216/wicd-xplico-261923.

9 http://sourceforge.net/projects/xplico/files/Xplico%20versions/version%200.6.2.

Figure 3 – Xplico VoIP decoding



mayhem. My short PCAP decoded resulted in three DNS hits, and five HTTP GETs.

NOTE: If you're using Xplico for analysis of malware-generated PCAPs, exercise the standard cautions. I recommend browsing the Xplico Web GUI from a VM for which you have snapshot. All results, particularly those specific to web sessions, are active hyperlinks and will send you to malicious command and control or infected sites when clicked.

This sample first hits whatsmyip.com (72.233.89.197) for obvious reasons (whoami), then conducts a geo-locate (whereami) from geoloc.daiguo.com (77.55.21.124), and finally phones home to 95.211.21.180, 182, and 184.

Under *Info* you can select *PCAP* and Xplico will provide you with a capture of just the selected conversation as seen in Figure 2.

You can view the HTTP request and response by clicking *GET* for the request/responses of interest.

This particular request included the AutoIt user-agent, a common indicator of the AutoIt Trojan,[10] another name for our Renocide/Harakit friend. By the way, anyone else for standardized malware naming conventions?

Experimenting with Xplico is an ideal time to create an account on Pcapr[11] and download PCAPs of your choosing. I was interested in captures that are inclusive of protocols I don't spend much time analyzing; particularly those that are VoIP related such as Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP). Even though the capture discussed below was posted to Pcapr, it seemed a bit of a privacy violation to post all the detail Xplico returns, including email address, IP address, and audio playback of the conversation (via Flash). As a result, I've redacted said details in Figure 3, but you'll definitely get a sense of how useful Xplico is.

If your duties include policy enforcement for your organization, or you work for law enforcement investigating the darkest of crimes, Xplico will also decode and render image files from web sessions.

Again, as we discussed above regarding malware analysis, be aware that Xplico will present you evidence in all its abhorrent detail. You're always at risk of seeing things you really never wanted to see.

That said, I grabbed a PCAP from Pcapr that results in a few harmless images via *Web => Images* as seen in Figure 4.

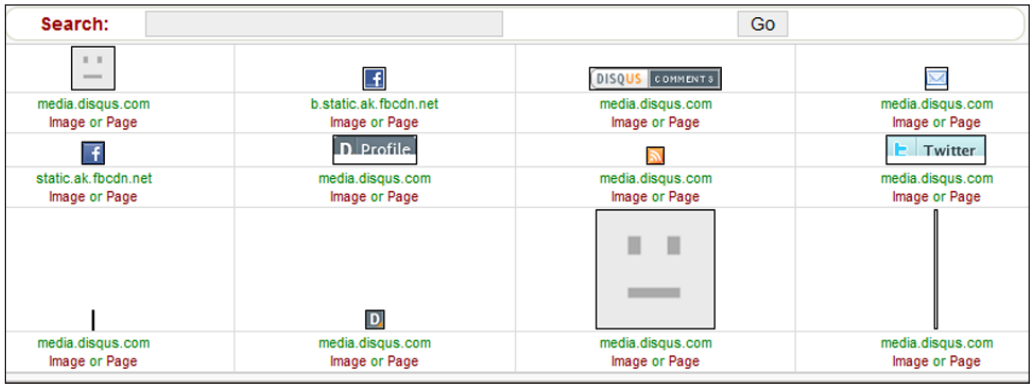


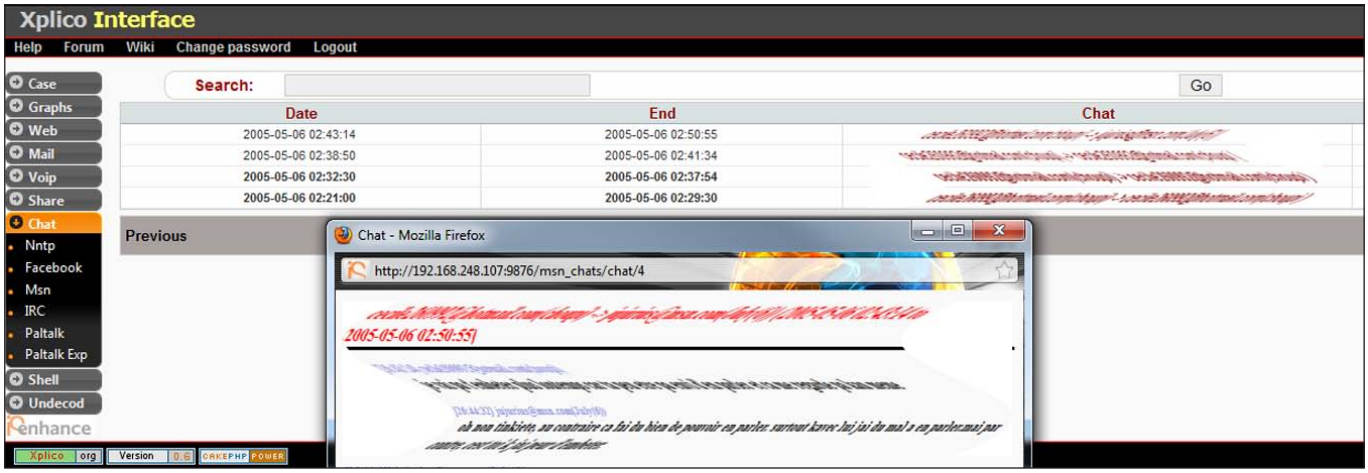
Figure 4 – Xplico image presentation

Similar evidence gathering activities may include the need to decode instant messaging captures. Xplico includes six chat-oriented decoders in the web GUI, but there are also l7-pattern classifiers for flows that aren't natively decoded includ-

10 http://www.secureworks.com/research/blog/trojans/20811.

11 http://pcapr.com.

Figure 5 – Xplico chat decoding



ing AIM, Jabber, and Skype, as well as others for gaming and core (DHCP, Netbios, NTP) flows. Figure 5 presents an MSN flow decoded; again, in the interest of privacy, I've obscured personally identifiable information.

Other features include the ability to generate a GeoMap (.kml file) that can be consumed by Google Maps and Google Earth. For command line aficionados Xplico can be used in console mode via the like of `./xplico -m pcap -f test.pcap`.

In conclusion

It's been a heck of year so far for *toolsmith*; we've discussed some consistently powerful (even scary) tools and Xplico is no exception. I highly suggest starting with PCAPs that interest you and see what Xplico uncovers. Just remember to be careful. There's lots of documentation and insight on the Xplico Wiki and Forum and you can look forward to consistent updates on the roadmap.[12]

12 http://www.xplico.org/roadmap

Enjoy this one!

Ping me via email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

Acknowledgements

—Gianluca Costa, project lead, for interview feedback

About the Author

Russ McRee, GCIH, GCFA, GPEN, CISSP, is team leader and senior security analyst for Microsoft's Online Services Security Incident Management team. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ at holisticinfosec dot org.