IP Fabrics: Network Forensic UI

May 15-06

Andy Heintz (Communications)

Altay Ozen (Team Lead)

Abe Devine (Webmaster)

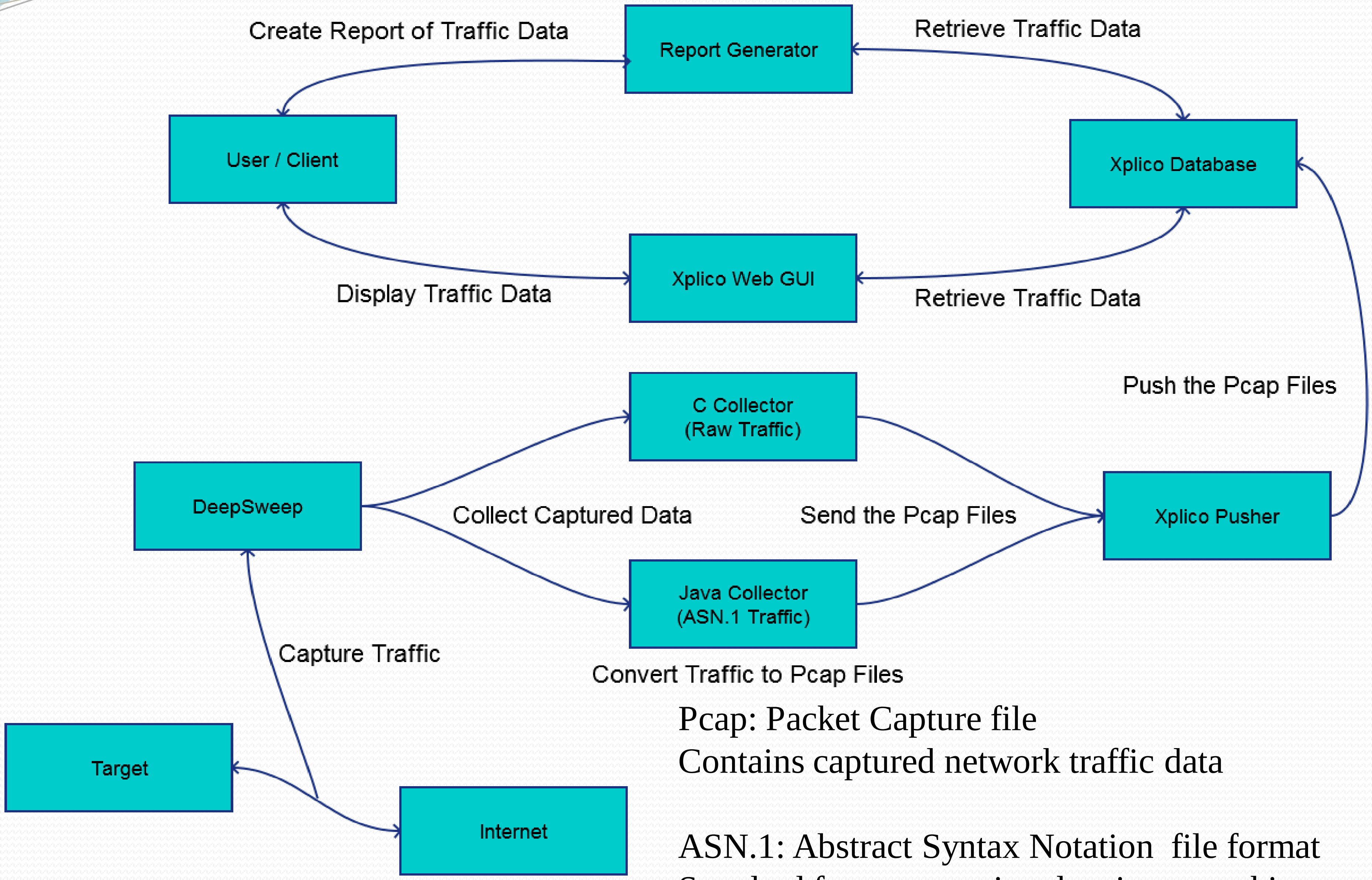
Client: Curt Schwaderer

Adviser: Dr. Joseph Zambreno

Problem Statement

- DeepSweep is a device for inspecting network traffic
- Does not have a GUI for viewing the output
- Xplico is a web UI for viewing network traffic
- Develop an interface between Xplico and DeepSweep

Design Diagram



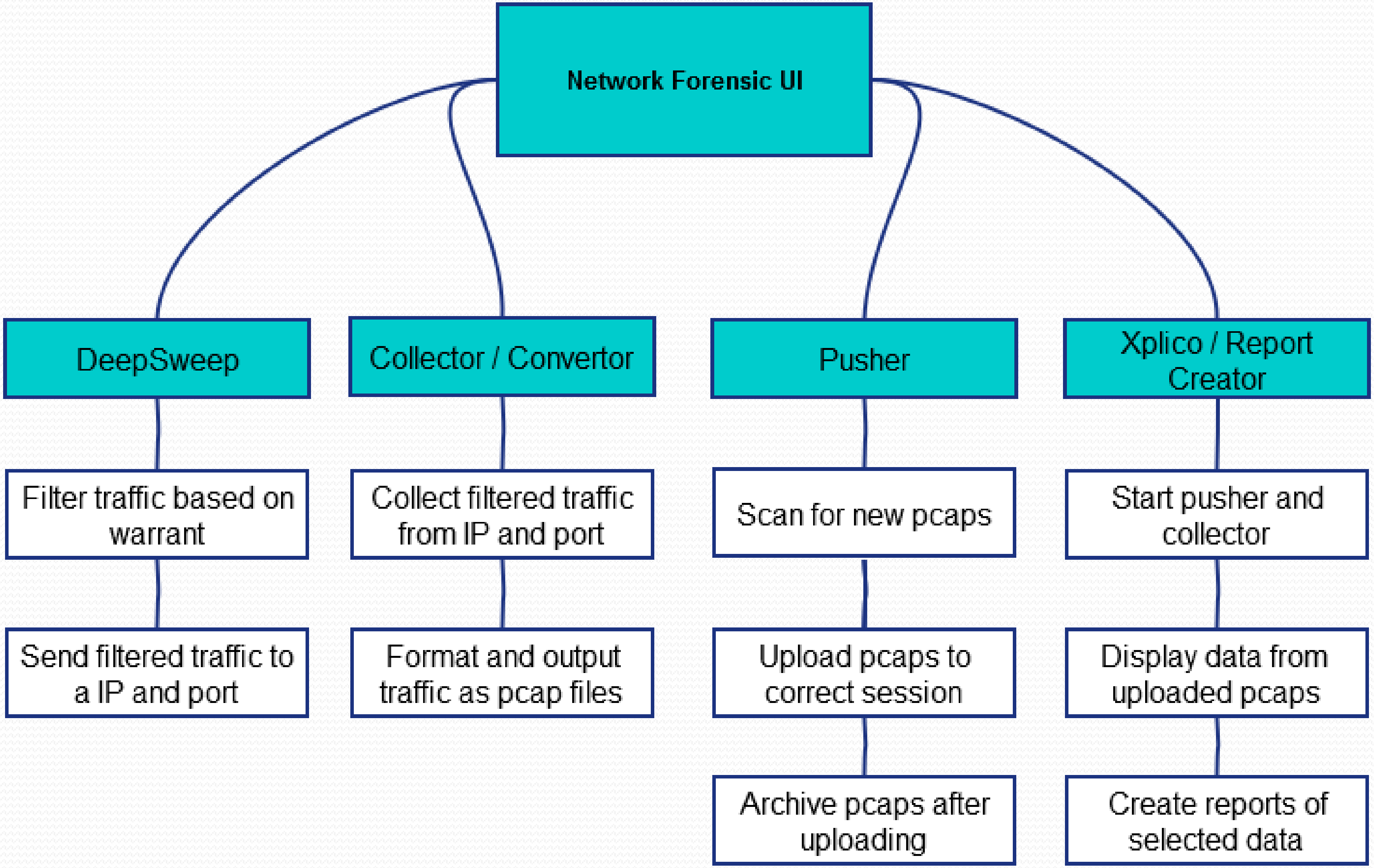
Pcap: Packet Capture file
Contains captured network traffic data

ASN.1: Abstract Syntax Notation file format
Standard for representing data in networking

Requirements

1. Xplico (modified): Start Pusher and the Collectors
2. C Collector (new): Create pcaps from raw traffic
3. Java Collector (new): Create pcaps from ASN.1 traffic
4. Xplico Pusher (existing): Upload new pcaps to Xplico
5. Xplico (existing): Display uploaded traffic in web GUI
6. Xplico (modified): Generate reports for traffic

Decomposition



Network Forensic UI
DeepSweep
Collector / Convertor
Pusher
Xplico / Report Creator
Filter traffic based on warrant
Send filtered traffic to a IP and port
Collect filtered traffic from IP and port
Format and output traffic as pcap files
Scan for new pcaps
Upload pcaps to correct session
Archive pcaps after uploading
Start pusher and collector
Display data from uploaded pcaps
Create reports of selected data

Non-Functional Requirements

- Reliability: Application should return information consistently and recover from errors.
- Maintainability: Documentation should be up-to-date and accurate; application should be easy to upgrade.
- Extensibility: Future developers should be able to easily add additional features using the existing architecture.

Software Specifications

- Languages: C, Java, Go, PHP, Python
- Collector (Raw Traffic): C
- Collector (ASN.1 Traffic): Java and Go
- Xplico: PHP, C, and Python
- Libraries: jnetpcap and TCPDF

Prototype

- Phase 1A: Handling Raw Traffic (C Collector)
- Phase 1B: Handling ASN.1 Traffic (Go Collector)
- Phase 2A: Replace Go Collector (Java Collector)
- Phase 2B: Extend Xplico (Report Generation)

User Interfaces

- Create Case and Session Pages: New option for start pcap uploads to the new case or session

- Case and Session Pages: New options for starting pcap uploads and generating reports

- Report Page: Displays list of generated reports

Potential Risks

- Xplico decodes pcaps slower than they are sent
- Raw traffic does not mark start / end of packet groups
- Xplico does not contain an API for extendibility

Test Plan

- Verify Pusher and Collector start correctly
- Test that Collectors create pcaps from collected traffic
- Verify data from pcaps is uploaded to Xplico
- Test that creating a report includes all the selected data
- Run regression tests after major changes
- Run integration and stress tests on system

Current Project Status

- Installed Xplico on Linux
- Finished research on project components
- Wrote and tested C Collector

Tasks and Responsibilities

- Altay Ozen: Team Lead and Collectors
- Andy Heintz: Documentation and Xplico Changes
- Abe Devine: Webmaster and Testing

Timeline

Phase 1A (Handling Raw Traffic)	Dec. 18
Phase 1B (Handling ASN.1 Traffic)	Feb. 20
Phase 2A (Replace Go Collector)	April 9
Phase 2B (Extend Xplico)	April 23

Questions?

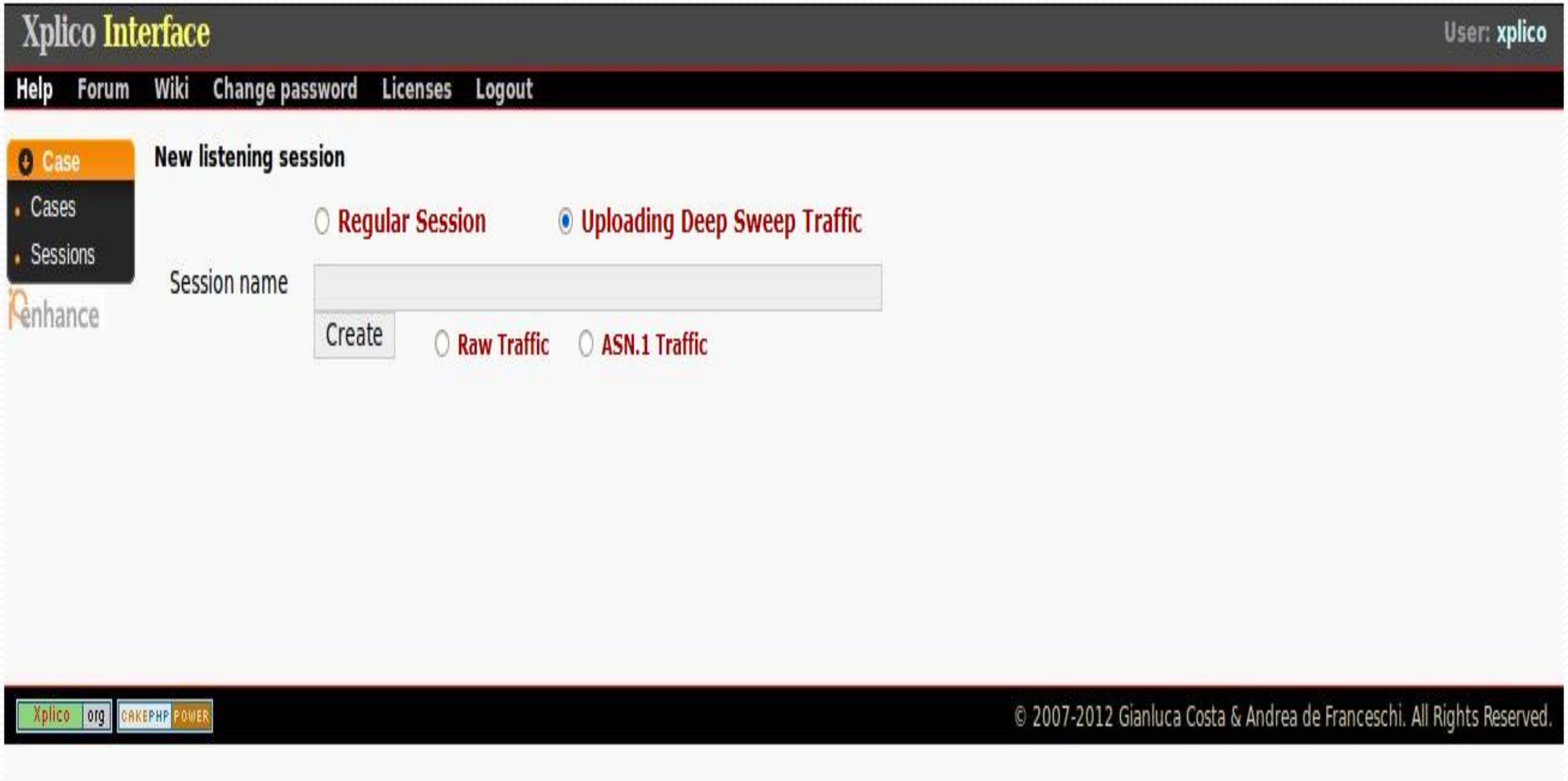
Inputs / Outputs

- Collector Input: Raw or ASN.1 traffic
- Collector Output: Pcap files

- Pusher Input: Pcap files
- Pusher Output: Data in Xplico’s database

- Xplico Input: Data in database
- Xplico Output: Traffic in GUI or report

New Session Page



New listening session

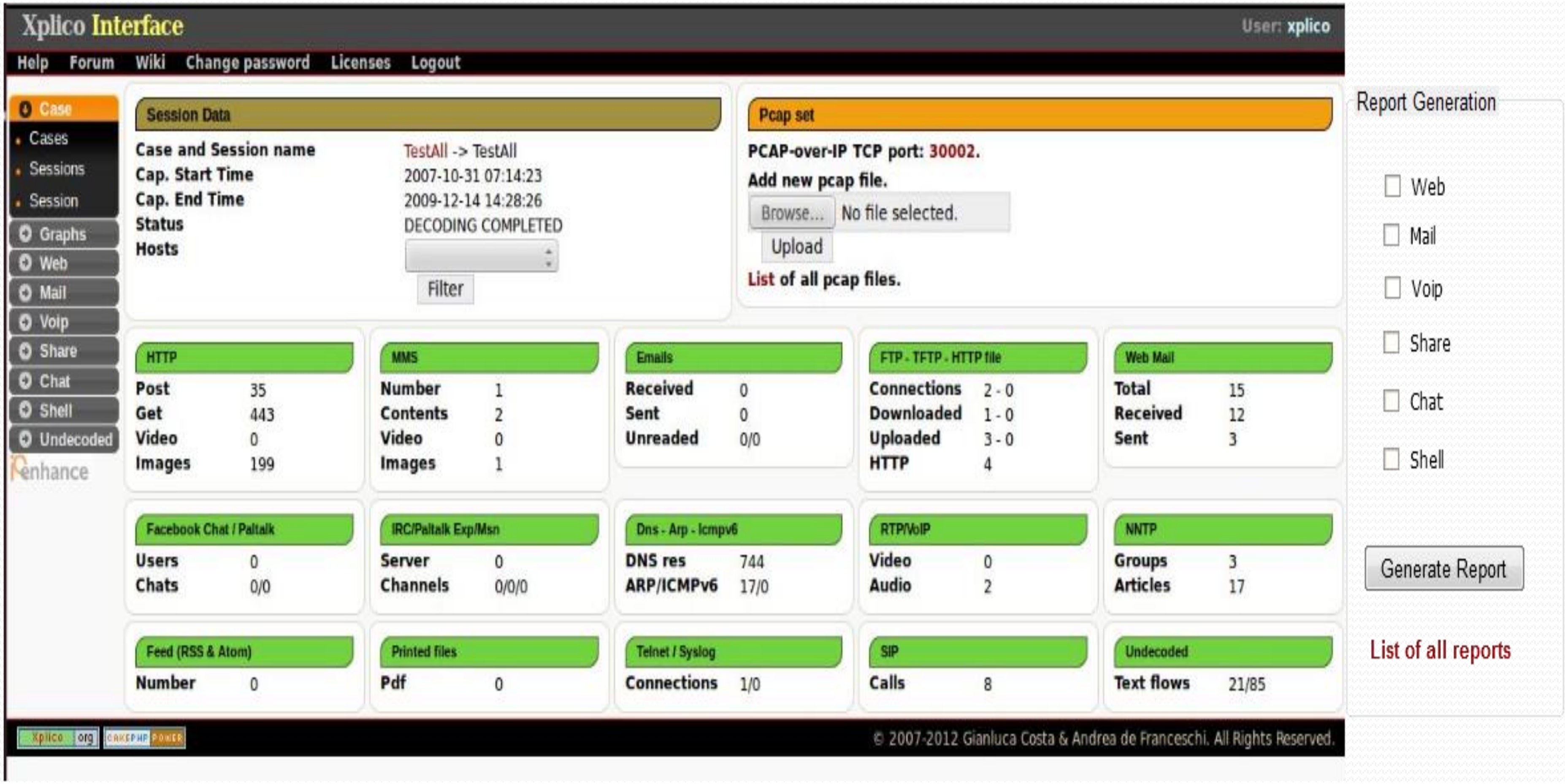
○ Regular Session ● Uploading Deep Sweep Traffic

Session name

○ Raw Traffic ○ ASN.1 Traffic

© 2007-2012 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Session Page



Session Data

Case and Session name	TestAll -> TestAll
Cap. Start Time	2007-10-31 07:14:23
Cap. End Time	2009-12-14 14:28:26
Status	DECODING COMPLETED
Hosts	

Pcap set

PCAP-over-IP TCP port: 30002.

Add new pcap file.

No file selected.

List of all pcap files.

HTTP

Post	35
Get	443
Video	0
Images	199

MMS

Number	1
Contents	2
Video	0
Images	1

Emails

Received	0
Sent	0
Unreaded	0/0

FTP - TFTP - HTTP file

Connections	2 - 0
Downloaded	1 - 0
Uploaded	3 - 0
HTTP	4

Web Mail

Total	15
Received	12
Sent	3

Facebook Chat / Paltalk

Users	0
Chats	0/0

IRC/Paltalk Exp/Msn

Server	0
Channels	0/0/0

Dns - Arp - Icmpv6

DNS res	744
ARP/ICMPv6	17/0

RTP/VoIP

Video	0
Audio	2

NNTP

Groups	3
Articles	17

Feed (RSS & Atom)

Number	0

Printed files

Pdf	0

Telnet / Syslog

Connections	1/0

SIP

Calls	8

Undecoded

Text flows	21/85

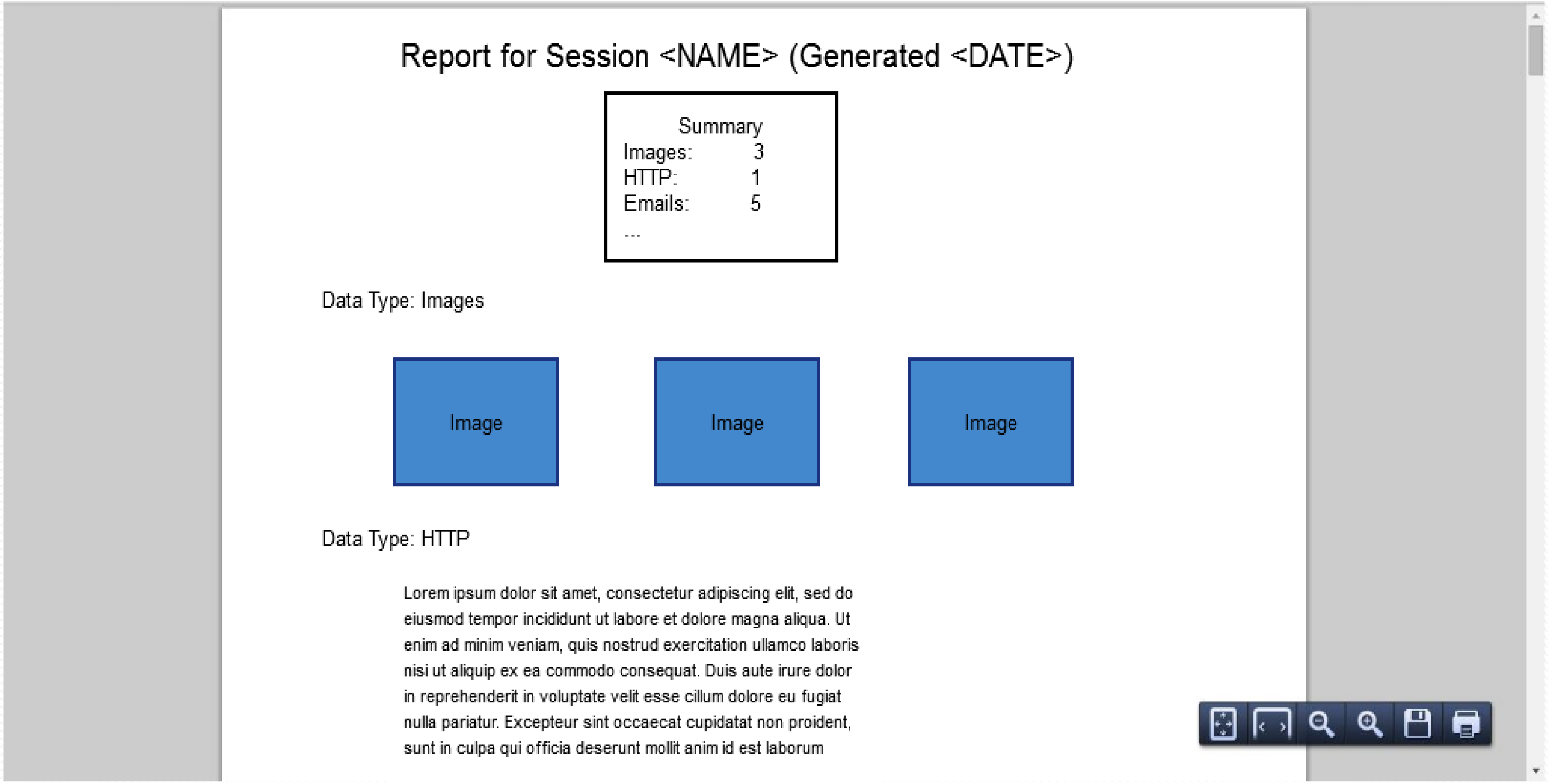
Report Generation

- ☐ Web
- ☐ Mail
- ☐ Voip
- ☐ Share
- ☐ Chat
- ☐ Shell

List of all reports

© 2007-2012 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Sample Report



Report for Session <NAME> (Generated <DATE>)

Summary

Images:	3
HTTP:	1
Emails:	5
...	

Data Type: Images

Data Type: HTTP

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum