



POSEIDON

IMC – Internet Monitoring Center
Internet Protocol (IP)

- Recording
- Reconstruction
- Evaluation

POSEIDON

IMC – Internet Monitoring Center
Internet Protocol (IP)



Table of Content

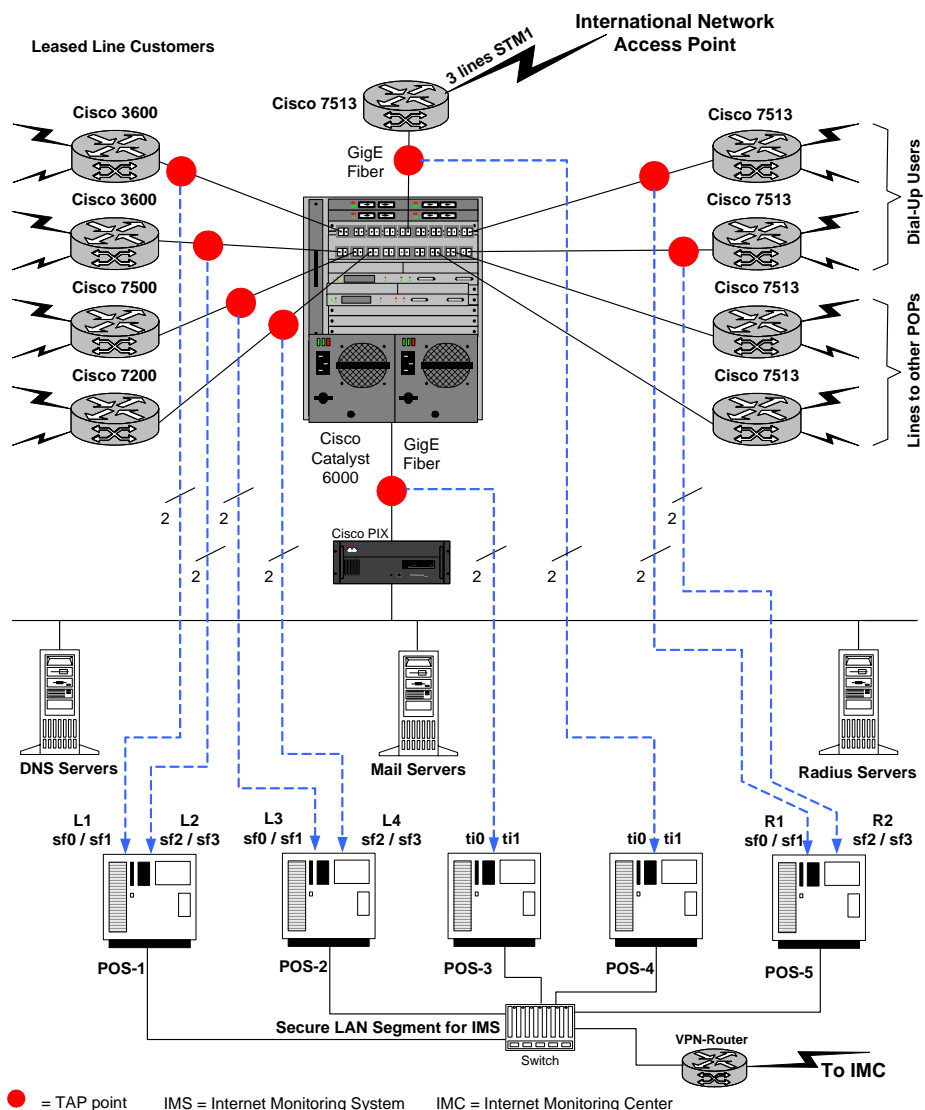
1	About POSEIDON.....	3
2	System Overview	4
3	Functional Description	6
3.1	Interface-Boards.....	6
3.2	Supported Network Protocols	6
3.3	Management Interface	7
3.4	Filter	7
4	Reconstruction of recorded IP-data.....	8
4.1	Reconstruction of a HTTP-Session	9
4.2	Reconstruction of emails	10
4.3	Reconstruction of FTP-Sessions.....	11
4.4	Reconstruction of Voice over IP Sessions (VoIP).....	12
4.5	Reconstruction of Chat-Sessions.....	13
5	Configurations.....	14
6	Connecting POSEIDON	14
7	Abbreviations	16
	Annex: Poseidon Supported Protocols	18

1. About POSEIDON

POSEIDON is an equipment for recording, reconstruction and evaluation of IP-Data, which are passively recorded from different communication lines.

It reads the data, filters them according to predefined filter criteria (depending on the way of using **POSEIDON** and the specific regulations within a country), adds a timestamp to the data (NTP-Server) and saves the data in raw format in a database. Using the Analyzer User Interface the data can – even online – be reconstructed and evaluated. For archiving purposes the saved raw data can automatically or manually be exported via FTP to already existing archiving media. Re-importing of archived raw data is also possible.

Connections and POSEIDON at a Big-ISP Site

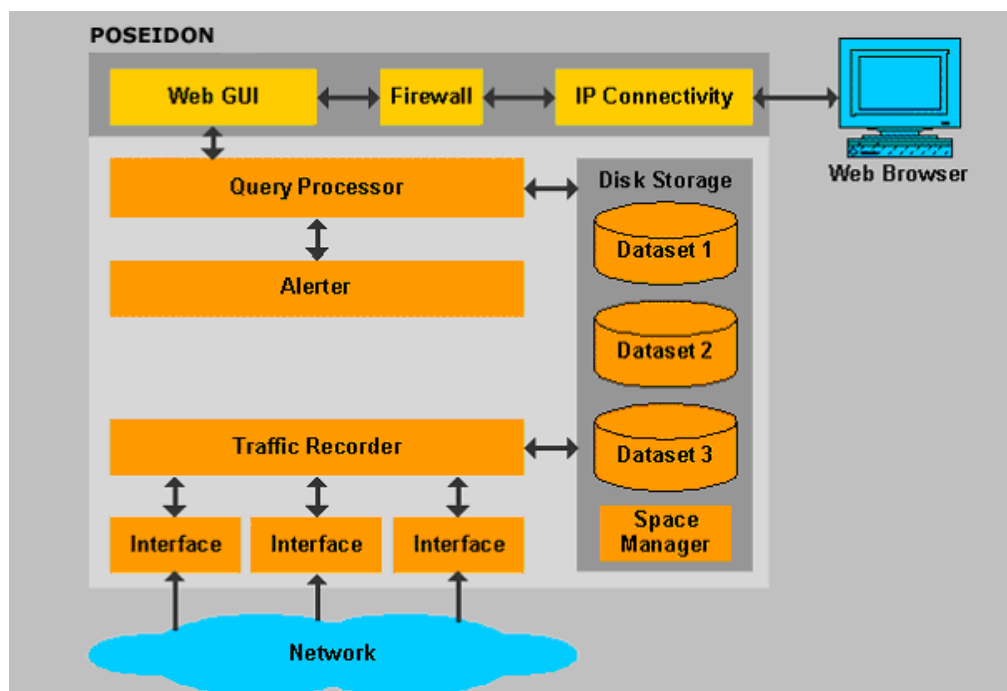


Pic. 1: POSEIDON – operating environment

2. System Overview

POSEIDON consists of 3 functional parts:

- Saving raw data, which are recorded from different communication links
- Database Management
- Reconstruction of IP-based data



Pic. 2: POSEIDON – System Overview

IP-data can be received by **POSEIDON** via a wide range of communication interfaces and it has the ability to record directly from the communication lines.

Important: All of the available interfaces are passive – that means they are only able to receive data and can not transmit any data. For that reason **POSEIDON** is totally invisible in a communication network and can not be identified.

The received IP-data are handed over from the interface(s) to the Recorder-Task, time-stamped and saved in the database. In parallel statistic data are generated for the data and also saved without manipulation of the raw data.

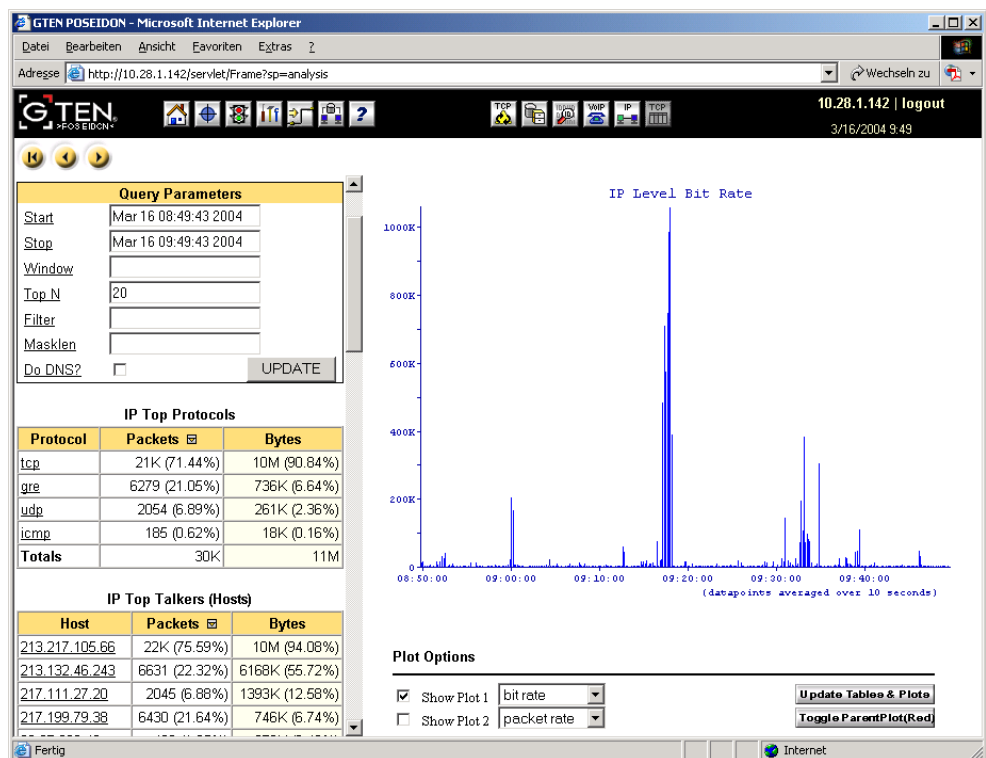
The Database Manager organizes the saved data, timestamps and statistics and provides the data to the Query-Processor and GUI-Server for reconstruction.

For reconstruction MS Internet Explorer is used, which can access **POSEIDON** via the integrated Ethernet Management Interface. The Internet Explorer is connected to the Web-Server, which provides the GUI for reconstructing the data. By using simple mouse clicks requests are transmitted to the database and the Query-Processor reads the required data, transfers it to the GUI-Server which is responsible for presenting the results of the reconstruction process via the Internet Explorer.

For the user an administration and reconstruction GUI is available. (see Pic. 3 and Pics in chapter 5 of this document).

The GUI is used for configuration of the interfaces and case oriented tasks, user administration, alarm management, data export and –import towards other systems and finally for reconstructing the IP-data.

The GUI provides a sophisticated search function which makes it possible to search for characters or character combinations within the complete TCP-communication. The results of a search process are presented as a list which shows all of the communication according to applications (e.g. email, HTTP-sessions, FTP, Telnet etc.) where the defined characters were found. Via a mouse click the listed applications can be reconstructed and displayed.



Pic. 3: POSEIDON – Graphical User Interface (GUI)

3. Functional Description

3.1 Interface-Boards

To receive IP-data via different communication links or networks **POSEIDON** was developed as a modular system. Depending on the requirements different interface boards can be integrated, which all are “receive only”.

The following interfaces are available:

- 10/100 Mbit/s Ethernet with 1, 2 or 4 ports
- 10/100/1000 Mbit/s Ethernet (Copper)
- Gigabit Ethernet 1000 Mbit/s (Fiber)
- T1 for 2 or 4 full duplex (FDX) connections
- E1 for 2 or 4 full duplex (FDX) connections
- FDDI (UTP or Multi-Mode-Fiber) for 1 full duplex (FDX) connection
- V.35 for 2 or 4 full duplex (FDX) connections
- X.21 for 2 or 4 full duplex (FDX) connections
- HSSI for 1 full duplex (FDX) connection
- T3 (Coax) for 1 full duplex (FDX) connection
- E3 (Coax) for 1 full duplex (FDX) connection
- OC-3 (SMF or MMF) for ATM
- OC-3 (SMF or MMF) for POS
- OC-12 (SMF or MMF) for ATM
- OC-12 (SMF or MMF) for POS

3.2 Supported Network Protocols

Depending on the requirements **POSEIDON** is able to filter and/or reconstruct IP-data according to the following protocols:

The following protocols (according to OSI 7 Layer Model) are supported:

- Link-Layer
 - Frame Relay
 - HDLC
 - CISCO HDLC
 - PPP
 - Bay PPP
 - MLPPP
 - 802.3/VLAN
- Network-Layer
 - IP
 - ATM and IP
 - POS and IP
 - WCP Compression
 - STAC Compression

3.3 Management Interface

The management of **POSEIDON**, which means configuring the system and the set-up of "criminal cases", is done via the built-in 10/100 Mbit/s network interface card (NIC). A stand-alone notebook or PC can be connected with a standard cross-connect LAN-cable or **POSEIDON** can be integrated in an already existing LAN of another Monitoring System via a HUB or Switch.

The basic IP-configuration (IP-Addresses, Subnet-Mask, Default-Gateway) can be performed with the integrated serial Console-Interface or with a keyboard and monitor directly connected to **POSEIDON**.

After its basic configuration **POSEIDON** can be connected to a network or stand-alone PC and all the additional configuration is performed with MS Internet Explorer. The access to **POSEIDON** can be granted – depending of the set-up of the firewall – for the following applications:

- HTTP or HTTPS for system configuration, reconstruction of IP-data, export and import of data.
- Telnet for access to the operating system for changing interface boards and for shutdown of the system.
- FTP for data export / -import

3.4 Filter

Depending on the way **POSEIDON** shall be used there are two different possibilities to handle IP-data:

- Filtering **prior** to recording/storing the IP-data
According to the filter set-up, incoming IP-data are checked and only data meeting the filter criteria will be recorded/stored.
- Filtering **after** recording/storing the IP-data
These settings have influence on the so called Query-Processor, when stored IP-data are reconstructed.

Filter expressions are created by combining so called **Qualifiers**. There are four kind of qualifiers:

- **Protocol Qualifier**
(Ethernet, FDDI, IP, ARP, RARP, TCP and UDP)
- **Direction Qualifier**
(Source, Destination, Source and Destination, Source or Destination)
- **Type Qualifier**
(Host-Name, IP-Address [range incl. subnet-mask], MAC, Port, Protocol,
link on serial interface [T1/E1; T3/E3],
channel on serial interface [T1/E1;T3/E3], DLCI, VPI and VCI [ATM],
number of VLAN)
- **ID Qualifier**
(Integer, IP-Address, MAC-Address, Protocol Name, Host Name)

For Example "**IP DST HOST 10.0.0.5**" means:

Filter all IP-traffic with the Destination for the HOST 10.0.0.5

4. Reconstruction of recorded IP-data

Reconstruction and evaluation of recorded IP-data can be started on each level of the involved protocol layer, e.g.:

- **PPP** (reconstruction as ASCII and/or HEX)
 - PAP
 - IPCP
 - LCP

- **Ethernet** (reconstruction as ASCII and/or HEX)

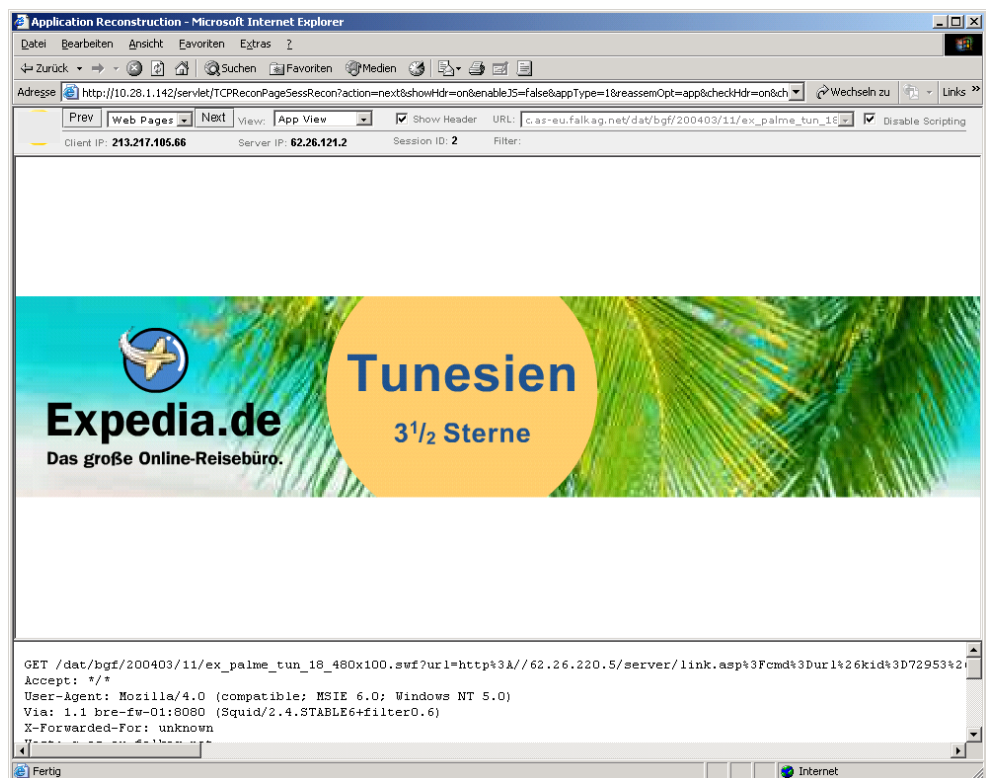
- **IP** (reconstruction as ASCII and/or HEX)
 - ICMP
 - UDP
 - TCP

- **TCP** (reconstruction according to the used application; also possible as ASCII, to make the complete TCP-Session visible)
 - SMTP
 - POP3
 - HTTP
 - IMAP4
 - Telnet
 - Chat
 - IRC
 - FTP
 - VoIP

The following chapters will use examples of reconstructed HTTP (www), email, FTP, VoIP and Chat sessions, to show how **POSEIDON** presents recorded IP-data for evaluation purposes.

4.1 Reconstruction of a HTTP-Session

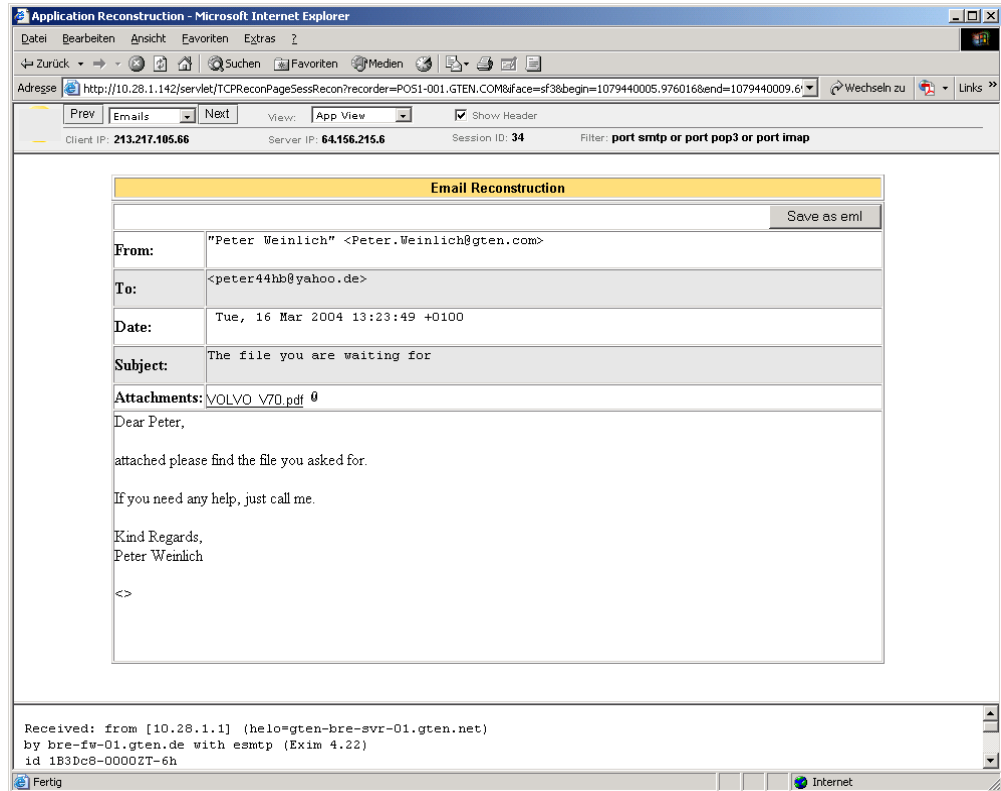
Picture 4 shows, how a recorded and reconstructed HTTP-Session is presented to the user for evaluation. The content of the page is shown in the same way like it was transmitted towards the monitored user via the communication network.



Pic. 4: POSEIDON – reconstructed Internet-page

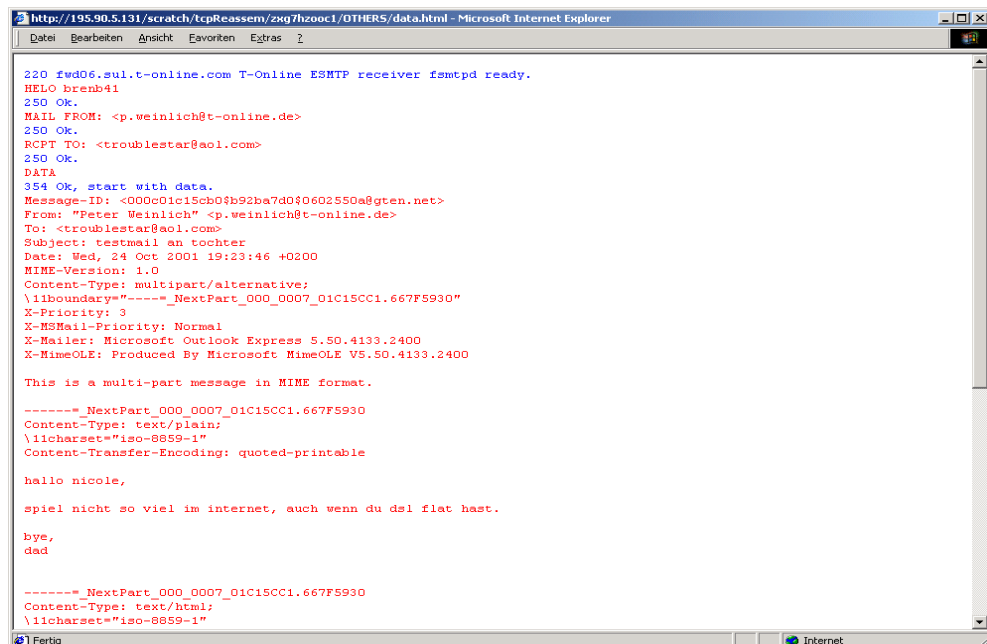
4.2 Reconstruction of emails

POSEIDON lists emails selected by incoming (POP3) and outgoing (SMTP) emails. Picture 5 shows an email with email-header and with attachment.



Pic. 5: POSEIDON –reconstructed email (Header and Content; Attachment)

Picture 6 shows the start of an email in ASCII-format, which can be used e.g. to evaluate a complete SMTP-Session.



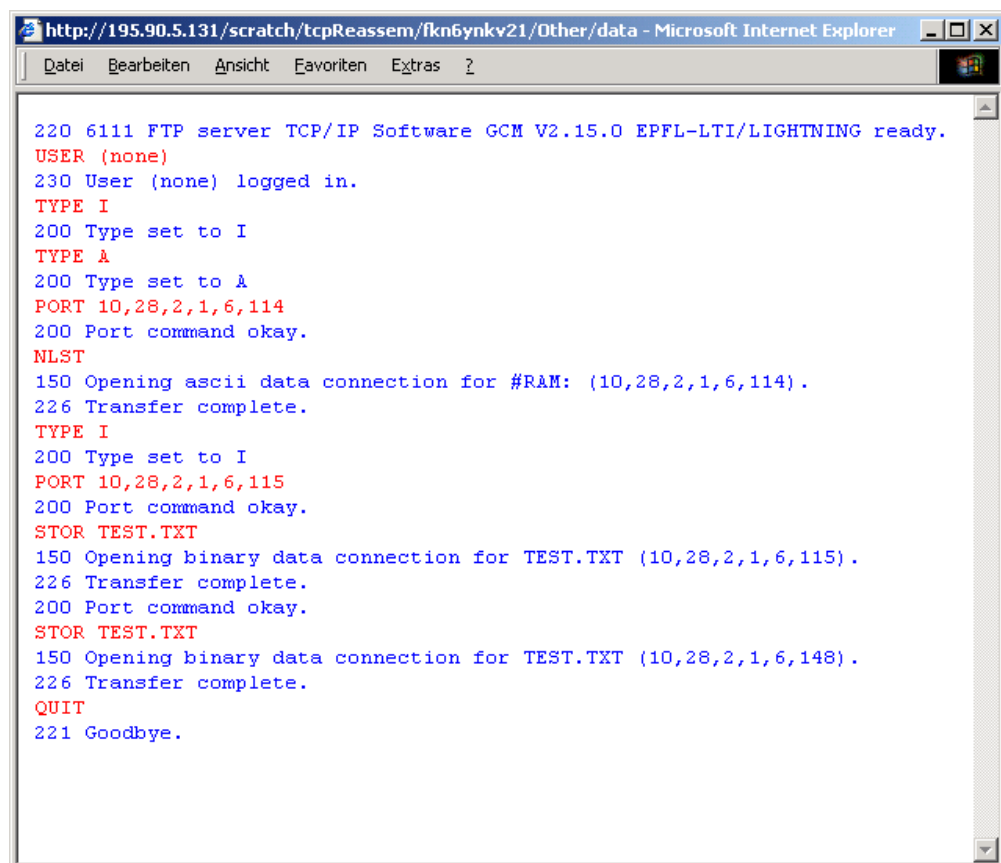
Pic. 6: POSEIDON –reconstructed email (in ASCII with the start of the SMTP-Session)

4.3 Reconstruction of FTP-Sessions

The reconstruction of character-based applications is done in ASCII-format.

The Server part of the communication is displayed in blue color, the Client's part in red (see Picture 10). Doing it this way makes it very easy for the evaluator to follow the complete session with all the requests and responses between Client and Server.

File transferred during the session with the commands „put“ or „get“ will be separated from the session. This makes it possible to reconstruct these file with appropriate applications like it is done with files attached to emails.



```

http://195.90.5.131/scratch/tcpReassem/fkn6ynkv21/Other/data - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?

220 6111 FTP server TCP/IP Software GCM V2.15.0 EPFL-LTI/LIGHTNING ready.
USER (none)
230 User (none) logged in.
TYPE I
200 Type set to I
TYPE A
200 Type set to A
PORT 10,28,2,1,6,114
200 Port command okay.
NLST
150 Opening ascii data connection for #RAM: (10,28,2,1,6,114).
226 Transfer complete.
TYPE I
200 Type set to I
PORT 10,28,2,1,6,115
200 Port command okay.
STOR TEST.TXT
150 Opening binary data connection for TEST.TXT (10,28,2,1,6,115).
226 Transfer complete.
200 Port command okay.
STOR TEST.TXT
150 Opening binary data connection for TEST.TXT (10,28,2,1,6,148).
226 Transfer complete.
QUIT
221 Goodbye.
  
```

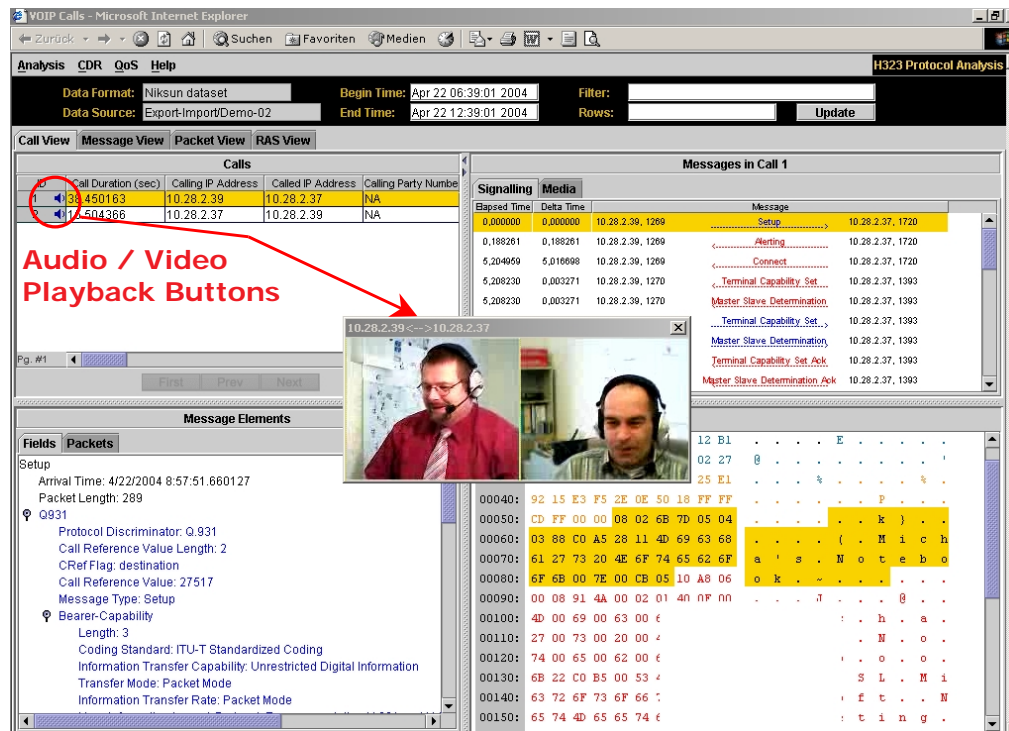
Pic. 7: POSEIDON – reconstructed FTP-Session (Server blue; Client red)

4.4 Reconstruction of Voice over IP Sessions (VoIP)

The reconstruction of VoIP-Sessions will provide the user with all relevant parts of the session, presented in ASCII and HEX.

With speakers or a headset connected to the evaluating computer, the voice content can be replayed.

Like with all of the above mentioned reconstructions, you all IP-addresses and – if applicable – the phone-numbers of the called and / or calling parties are shown for evaluation purposes.

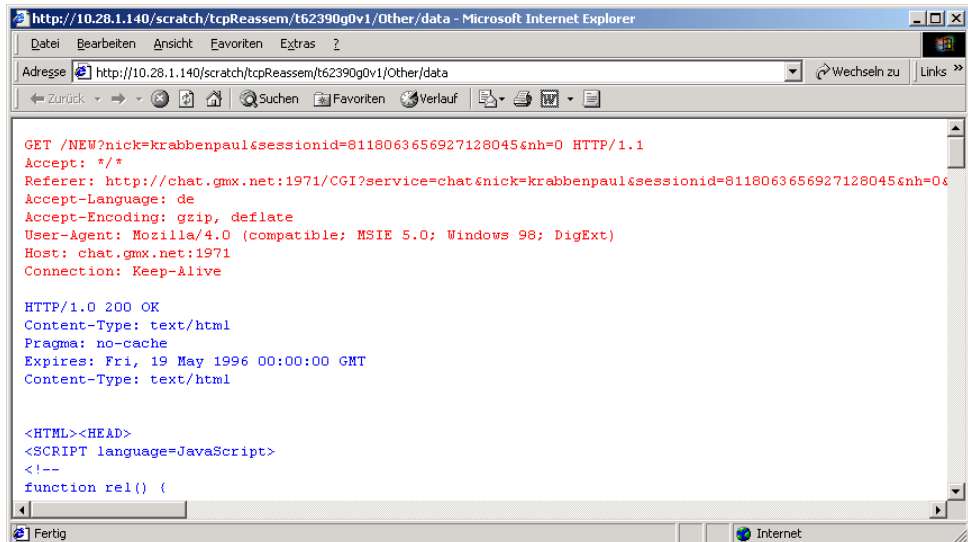


Pic. 8: POSEIDON – reconstructed VoIP-Session (with video – MS NetMeeting)

4.5 Reconstruction of Chat-Sessions

A reconstructed Chat-Session can be made visible in ASCII- or HTML-format. Using the ASCII presentation, the Client's part of the communication is displayed in red, the Server's part in blue color.

Using HTML-format, a Chat-Session is displayed with all participants of the chat in different colors, which makes it very convenient for the evaluator, to find a specific user.



```

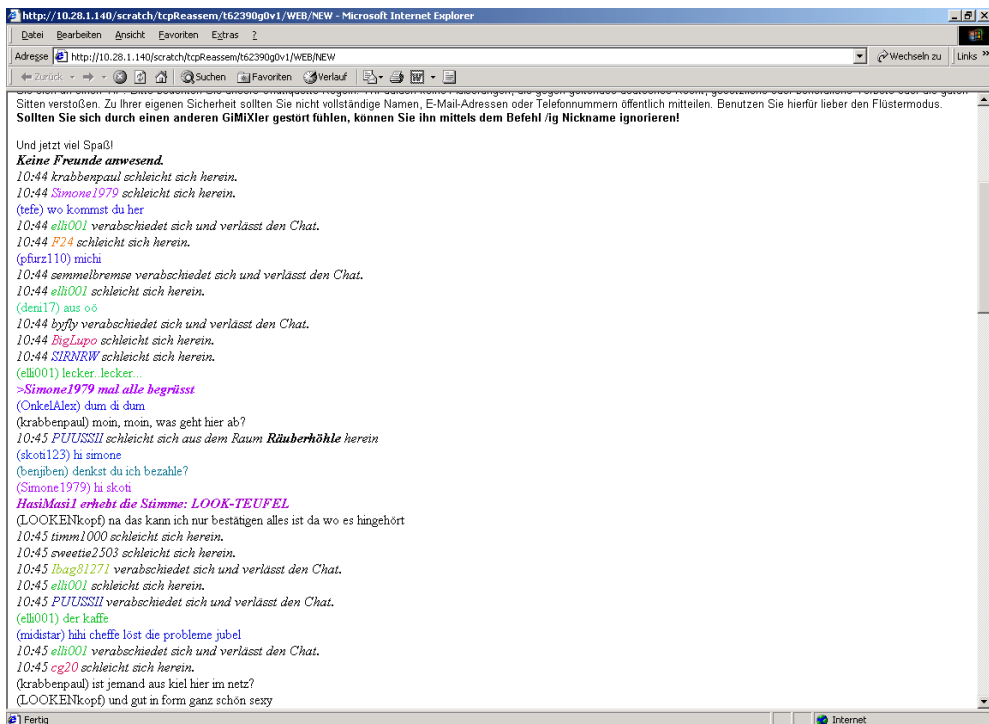
http://10.28.1.140/scratch/tcpReassem/t62390g0v1/Other/data - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Adresse http://10.28.1.140/scratch/tcpReassem/t62390g0v1/Other/data
Zurück Suchen Favoriten Verlauf
GET /NEW?nick=krabbenpaul&sessionId=8118063656927128045&nh=0 HTTP/1.1
Accept: */*
Referer: http://chat.gmx.net:1971/CGI?service=chat&nick=krabbenpaul&sessionId=8118063656927128045&nh=0
Accept-Language: de
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)
Host: chat.gmx.net:1971
Connection: Keep-Alive

HTTP/1.0 200 OK
Content-Type: text/html
Pragma: no-cache
Expires: Fri, 19 May 1996 00:00:00 GMT
Content-Type: text/html

<HTML><HEAD>
<SCRIPT language=JavaScript>
<!--
function rel() {

```

Pic. 9: POSEIDON – reconstructed Chat-Session (in ASCII)



```

http://10.28.1.140/scratch/tcpReassem/t62390g0v1/WEB/NEW - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Adresse http://10.28.1.140/scratch/tcpReassem/t62390g0v1/WEB/NEW
Zurück Suchen Favoriten Verlauf
Sitten verstoßen. Zu Ihrer eigenen Sicherheit sollten Sie nicht vollständige Namen, E-Mail-Adressen oder Telefonnummern öffentlich mitteilen. Benutzen Sie hierfür lieber den Flüstermodus.
Sollten Sie sich durch einen anderen GIMIXler gestört fühlen, können Sie ihn mittels dem Befehl /ig Nickname ignorieren!

Und jetzt viel Spaß!
Keine Freunde anwesend.
10:44 krabbenpaul schleicht sich herein.
10:44 Simone1979 schleicht sich herein.
(tefe) wo kommst du her
10:44 elh001 verabschiedet sich und verlässt den Chat.
10:44 F24 schleicht sich herein.
(pfuz110) michi
10:44 semmelbremse verabschiedet sich und verlässt den Chat.
10:44 elh001 schleicht sich herein.
(deta17) aus oö
10:44 byffy verabschiedet sich und verlässt den Chat.
10:44 BigLupo schleicht sich herein.
10:44 SIRNRW schleicht sich herein.
(elh001) lecker. lecker...
->Simone1979 mal alle begrüsst
(OnkelAlex) dum di dum
(krabbenpaul) moin, moin, was geht hier ab?
10:45 PUUSSII schleicht sich aus dem Raum Rüberhöhle herein
(skoti23) hi simone
(benjben) denkst du ich bezahle?
(Simone1979) hi skoti
HasiMasi1 erhebt die Stimme: LOOK-TEUFEL
(LOOKENkopf) na das kann ich nur bestätigen alles ist da wo es hingehört
10:45 timm1000 schleicht sich herein.
10:45 sweetie2503 schleicht sich herein.
10:45 Jbag81271 verabschiedet sich und verlässt den Chat.
10:45 elh001 schleicht sich herein.
10:45 PUUSSII verabschiedet sich und verlässt den Chat.
(elh001) der Kaffe
(madstar) häh cheffe löst die probleme jubel
10:45 elh001 verabschiedet sich und verlässt den Chat.
10:45 cg20 schleicht sich herein.
(krabbenpaul) ist jemand aus kiel hier im netz?
(LOOKENkopf) und gut in form ganz schön sexy

```

Pic. 10: POSEIDON – reconstructed Chat-Session (in HTML)

5. Configurations

Description	1U Chassis	2U Chassis	5U Chassis
Max storage Capacity	292 GB	876 GB	1.168 MB
RAID-Controller	optional	optional	X
Fast Ethernet monitoring	X	X	X
Gigabit Ethernet monitoring	no	X	X
T1/E1 monitoring	no	X	X
T3/E3 monitoring	no	X	X
V.35/X.21 monitoring	no	X	X
FDDI/HSSI monitoring	no	X	X
OC-3 monitoring (Optical Carrier 155 Mbit/s, ATM or POS networks)	no	X	X
OC-12 monitoring (Optical Carrier 622 Mbit/s, ATM or POS networks)	no	X	X
Multi-Interface monitoring	no	X	X
VoIP monitoring	X	X	X

6. Connecting POSEIDON

To connect **POSEIDON** to the communication lines or networks for recording the transmitted IP-data so called **Taps** will be used.

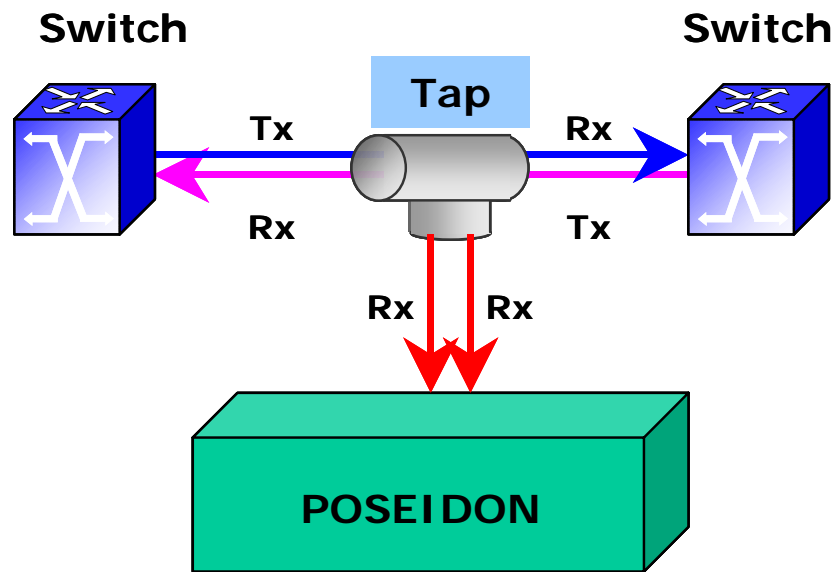
Taps or Splitters are some kind of „T-connectors“, which are tapped into the communication line and duplicate the transported data signals 1:1 and transfer them to the **POSEIDON** for recording. It is important, that the communication between transmitter and receiver will not be interfered.

Using Taps means:

- The Taps have to be installed physically into the communication line
- Taps will attenuate the signals on the line, which has to be taken into account
- Taps will work in duplex mode, but only one-way, which means they are passive devices
- A breakdown of a Tap or its power-supply will not effect the monitored communication

Taps are available for different lines / interfaces and will be delivered together with the appropriate interface boards.

Picture 11 shows how a Tap works in principle.



Pic. 11: POSEIDON –connected with a Tap

POSEIDONs with 2 or 4 ports FDX (Full Duplex) are used to be connected with **TAPs**

(Tx and Rx on physically split connections).

With 2 ports one single and with 4 ports two of these connections can be established.

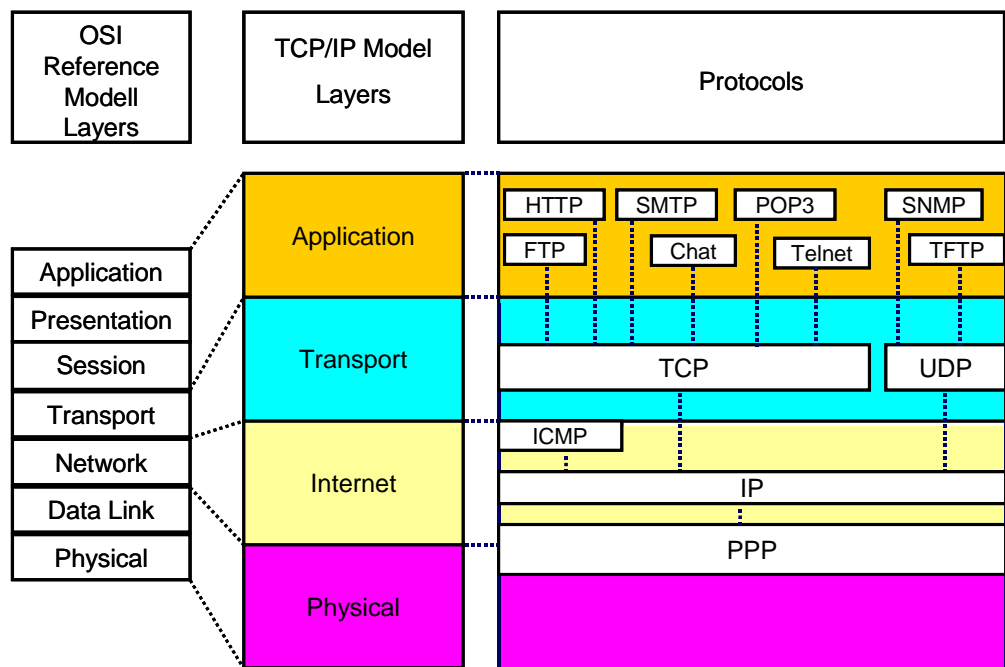
POSEIDONs with 1, 2 or 4 ports HDX (Half Duplex) are used to be connected with **HUBs** or **SPAN**-ports (Tx and Rx on the same physical connection).

With 1 port one single, with 2 ports two and with 4 ports four of these connections can be established.

7. Abbreviations

ADSL	Asymmetrical Digital Subscriber Line		
ATM	Asynchronous Transfer Mode, data rate 25 - 622 Mbps.		
Chat	Real time communication, e.g. Internet by using characters - IRC		
COLP	Connected Line Presentation		
CUG	Closed User Group		
DB	Data base		
DSL	Digital Subscriber Line (xDSL)		
E1	European Digital Signal Level No. 1, 2048 kbit/s, 30 channels, 64 kbit/s each		
E3	European Digital Signal Level No. 3, 34.368 Mbit/s, 16x E1-channels, 480 channels, 64 kbit/s each		
FDDI	Fiber Distributed Data Interface		
FTAM	File Transfer, Access and Management		
FTP	File Transfer Protocol		
GPS	Global Positioning System		
GUI	Graphical User Interface		
HI	Handover Interface		
HI2	Hand Over Interface Layer 2		
HI3	Hand Over Interface Layer 3		
HSSI	High Speed Serial Interface		
HTTP	Hypertext Transfer Protocol		
HTTPS	HTTP Secure		
ICMP	Internet Control Message Protocol		
IMAP	Internet Message Access Protocol		
IP	Internet Protocol		
IP-data	Data based on IP, generated by e.g. PC, GPRS, UMTS etc.		
IRC	Internet Relay Chat		
ITU	International Telecommunication Union		
LAN	Local Area Network		
LEA	Law Enforcement Agency		
LI	Lawful Interception		
MMF	Multi Mode Fiber		
NNTTP	Network News Transfer Protocol		
OC	Optical Carrier (using electrical transmission with wire also called STS (Synchronous Transport Signal))		
OC-1	Data rate:	51,84 Mbit/s	STS 1
OC-3	Data rate:	155.52 Mbit/s	STS 3
OC-9	Data rate:	466.56 Mbit/s	STS 9
OC-12	Data rate:	622.08 Mbit/s	STS 12
OC-18	Data rate:	933.12 Mbit/s	STS 18
OC-24	Data rate:	1.244 Gbit/s	STS 24
OC-36	Data rate:	1.866 Gbit/s	STS 36
OC-48	Data rate:	2.48832 Gbit/s	STS 48
OC-96	Data rate:	4.976 Gbit/s	STS 96
OC-192	Data rate:	9.952 Gbit/s	STS 192
OC-768	Data rate:	40.6 Gbit/s	STS 768
PC	Personal Computer		
PDU	Protocol Data Unit		
POP3	Post Office Protocol 3		
POS	Packet over SONET		
SMF	Single Mode Fiber; also called Mono Mode Fiber		
SONET	Synchron Optical Network (see OC or STS)		
STM	Synchronous Transport Mode		
STM-1	STM Level 1	data rate:	155.52 Mbit/s
STM-2	STM Level 2	data rate:	207.36 Mbit/s

STM-3	STM Level 3	data rate:	476.56 Mbit/s
STM-4	STM Level 4	data rate:	622.08 Mbit/s
STM-6	STM Level 6	data rate:	933.12 Mbit/s
STM-8	STM Level 8	data rate:	1.24416 Gbit/s
STM-16	STM Level 16	data rate:	2.48832 Gbit/s
STM-32	STM Level 32	data rate:	4.976 Gbit/s
STM-64	STM Level 64	data rate:	9.95328 Gbit/s
STS	Synchronous Transport Signal, see OC		
T1,3	US format for digital transmission		
T1	data rate:	1.544Mbit/s	(24 channels 56 kbit/s each)
T3	data rate:	44.736 Mbit/s	(672 channels 56 kbit/s each); (27x T1)
TCP	Transmission Control Protocol		
Telnet	Terminal program (virtual terminal service)		
UDP	User Datagram Protocol		
URL	Uniform Resource Locator		
V.35	ITU Standard for synchronous high-speed data transmission		
WAN	Wide Area Network		
X.25	Standard for packet oriented networks		
xDSL	see DSL		



Graphic: TCP/IP-Layers and ISO/OSI-Reference Model (7 Layer)

POSEIDON

Supported Protocols

Application Reconstruction

Recording Interfaces

1. Supported Protocols

On the following pages you will find the protocols supported by POSEIDON in alphabetical order:

A

3GPP2 A11; ATM AAL1; ATM AAL3/4; Appletalk Address Resolution Protocol; Application Configuration Access Protocol; ACN; OSI ISO/IEC 10035-1 ACSE Protocol; AppleTalk Filing Protocol; Andrew File System (AFS); Authentication Header; AOL Instant Messenger; AIM Administrative; AIM Advertisements; AIM Privacy Management Service; AIM Buddylist Service; AIM Chat Service; AIM Chat Navigation; AIM Directory Search; AIM Generic Service; AIM ICQ; AIM Invitation Service; AIM Location; AIM User Lookup; AIM Messaging; AIM OFT; AIM Popup; AIM Signon; AIM Server Side Info; AIM Statistics; AIM Translate; Apache JServ Protocol v1.3; AAL type 2 signalling protocol - Capability set 1 (Q.2630.1); Intel ANS probe; ANSI IS-637-A (SMS) Teleservice Layer; ANSI IS-637-A (SMS) Transport Layer; ANSI IS-683-A (OTA (Mobile)); ANSI IS-801 (Location Services (PLD)); ANSI A-I/F BSMAP; ANSI A-I/F DTAP; ANSI Mobile Application Part; Ad hoc On-demand Distance Vector Routing Protocol; Apple IP-over-IEEE 1394; ARCNET; Address Resolution Protocol; Art-Net; Aggregate Server Access Protocol; Lucent/Ascend debug output; Alert Standard Forum; ASN.1 decoding; AppleTalk Session Protocol; ATM; AppleTalk Transaction Protocol packet; Microsoft Task Scheduler Service; Cisco Auto-RP

B

Building Automation and Control Network APDU; Building Automation and Control Network NPDU; PPP Bandwidth Allocation Control Protocol; PPP Bandwidth Allocation Protocol; Blocks Extensible Exchange Protocol; Basic Encoding Rules (ASN.1 X.690); Bi-directional Fault Detection Control Message; Border Gateway Protocol; Bearer Independent Call Control ; Wellfleet Breath of Life; Bootstrap Protocol; Boot Parameters; DCE/RPC BOS Server; Boardwalk; Microsoft Windows Browser Protocol; BSSAP/BSAP; BSS GPRS Protocol; DCE/RPC BUDB; DCE/RPC BUTC; BACnet Virtual Link Control

C

Cast Client Control Protocol; PPP Callback Control Protocol; PPP Compression Control Protocol; CCSDS; Cisco Discovery Protocol; PPP CDP Control Protocol; CDS Clerk Server Calls; DCE/RPC CDS Solicitation; Cisco NetFlow; Cisco Group Management Protocol; PPP Challenge Handshake Authentication Protocol; Cisco HDLC; Connectionless Lightweight Directory Access Protocol; Clearcase NFS; ISO 8473 CLNP ConnectionLess Network Protocol; ISO 8602 CLTP ConnectionLess Transport Protocol; PPP Compressed Datagram; DCE/RPC Conversation Manager; Common Open Policy Service; CoSine IPNOS L2 debug output; ISO 8073 COTP Connection-Oriented Transport Protocol; Cross Point Frame Injector ; Check Point High Availability Protocol; DNS Control Program Server; Common Unix Printing System (CUPS) Browsing Protocol

D

Data; Line-based text data; Distributed Checksum Clearinghouse Protocol; DFS Calls; DCE/RPC UpServer; DCE RPC; DICOM; Datagram Delivery Protocol; Dynamic DNS Tools Protocol; DEC Spanning Tree Protocol; Microsoft Distributed File System; DHCPv6; Diameter Protocol; Distcc Distributed Compiler; Data Link Switching; Domain Name Service; Windows 2000 DNS; DOCSIS 1.1; DOCSIS Baseline Privacy Key Management Attributes; DOCSIS Baseline Privacy Key Management Request; DOCSIS Baseline Privacy Key Management Response; DOCSIS Dynamic Service Addition Acknowledge; DOCSIS Dynamic Service Addition Request; DOCSIS Dynamic Service Addition Response; DOCSIS Dynamic Service Change Acknowledgement; DOCSIS Dynamic Service Change Request; DOCSIS Dynamic Service Change Response; DOCSIS Dynamic Service Delete Request; DOCSIS Dynamic Service Delete Response; DOCSIS Initial Ranging Message; DOCSIS Upstream Bandwidth Allocation; DOCSIS Mac Management; DOCSIS Registration Acknowledge; DOCSIS Registration Requests; DOCSIS Registration Responses; DOCSIS Range Request Message; DOCSIS Ranging Response; DOCSIS Appendix C TLV's; DOCSIS Upstream Channel Descriptor Type 29; DOCSIS Upstream Channel Change Request; DOCSIS Upstream Channel Change Response; DOCSIS Upstream Channel Descriptor; DOCSIS Vendor Specific Endodings; Microsoft Directory Replication Service; Data Stream Interface; DCE Distributed Time Service Provider; DCE Distributed Time Service Local Server; Distance Vector Multicast Routing Protocol

E

ITU-T E.164 number; Extensible Authentication Protocol; 802.1x Authentication; Echo; eDonkey Protocol; Microsoft Encrypted File System Service; Enhanced Interior Gateway Routing Protocol; FC Extended Link Svc; OpenBSD Encapsulating device; EtherNet/IP (Industrial Protocol); ENTTEC; DCE/RPC Endpoint Mapper;

DCE/RPC Endpoint Mapper4; ISO 9542 ESIS Routeing Information Exchange Protocol; Encapsulating Security Payload; Ethernet; Ethernet over IP

F

Fibre Channel; Fibre Channel Name Server; Fibre Channel Common Transport; FCIP; Fibre Channel Protocol for SCSI; FC Fabric Configuration Server; Fibre Channel Security Protocol; Fiber Distributed Data Interface; Financial Information eXchange Protocol; DCE/RPC FLDB; Frame Relay; Frame; OSI ISO 8571 FTAM Protocol; File Transfer Protocol (FTP); FTP Data; FTServer Operations; Checkpoint FW-1; Fibre Channel Fabric Zone Server

G

General Inter-ORB Protocol; Coseventcomm Dissector Using GIOP API; Cosnaming Dissector Using GIOP API; GARP Multicast Registration Protocol; Gnutella Protocol; GPRS Network service; Generic Routing Encapsulation; DG Gryphon Protocol; GSM Short Message Service User Data; GSM A-I/F BSSMAP; GSM A-I/F DTAP; GSM A-I/F RP; GSM Mobile Application Part; GSM SMS TPDU (GSM 03.40); Generic Security Service Application Program Interface; GPRS Tunnelling Protocol; GARP VLAN Registration Protocol

H

Sinec H1 Protocol; H225; H245; ITU-T Recommendation H.261; ITU-T Recommendation H.263 RTP Payload header (RFC2190); H4501; Hummingbird NFS Daemon; HP Extended Local-Link Control; Cisco Hot Standby Router Protocol; Hypertext Transfer Protocol; HyperSCSI

I

Information Access Protocol; Inter-Access-Point Protocol; IAX2; Interbase; Internet Content Adaptation Protocol; DCE/RPC ICL RPC; Internet Control Message Protocol; Internet Control Message Protocol v6; Internet Cache Protocol; ICQ Protocol; Internet Group membership Authentication Protocol; Internet Group Management Protocol; Cisco Interior Gateway Routing Protocol; ILMI; Comuserve GIF; JPEG File Interchange Format; Internet Message Access Protocol; Remote Shutdown; Internet Protocol; IP Payload Compression; PPP IP Control Protocol; IP Device Control (SS7 over IP); IP Over FC; Intelligent Platform Management Interface; Internet Printing Protocol; Internet Protocol Version 6; PPP IPv6 Control Protocol; IP Virtual Services Sync Daemon; Internetwork Packet eXchange; IPX Message; IPX Routing Information Protocol; Service Advertisement Protocol; IPX WAN; Internet Relay Chat; IrCOMM Protocol; IrDA Link Access Protocol; IrDA Link Management Protocol; Internet Security Association and Key

Management Protocol; iSCSI; ISDN; ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol; Cisco ISL; InterSwitch Message Protocol; iSNS; ISDN User Part; ISDN Q.921-User Adaptation Layer

J

Jabber XML Messaging

K

Kerberos Administration; Kerberos; Kernel Lock Manager; MS Kpasswd; DCE/RPC Kerberos V

L

Layer 2 Tunnelling Protocol; Link Aggregation Control Protocol; ATM LAN Emulation; Microsoft Windows Lanman Remote API Protocol; Link Access Procedure Balanced (LAPB); Link Access Procedure Balanced Ethernet (LAPBETHER); Link Access Procedure; Channel D (LAPD); Laplink; PPP Link Control Protocol; Lightweight Directory Access Protocol; Label Distribution Protocol; LocalTalk Link Access Protocol; DCE/RPC NCS 1.5.1 Local Location Broker; Logical-Link Control; Logical Link Control GPRS; Local Management Interface; Link Management Protocol (LMP); Log Message; Line Printer Daemon Protocol; Microsoft Local Security Architecture; Microsoft Local Security Architecture (Directory Services); LWAPP Encapsulated Packet; LWAPP Control Message; LWAPP Layer 3 Packet; Light Weight DNS RESolver (BIND9)

M

MTP2 Peer Adaptation Layer; MTP 2 Transparent Proxy; MTP 2 User Adaptation Layer; MTP 3 User Adaptation Layer; SMB MailSlot Protocol; Malformed Packet; Microsoft Exchange MAPI; Modbus/TCP; MDS Header; Media Type; MEGACO; Media Type: message/http; Microsoft Messenger Service; Media Gateway Control Protocol; DCE/RPC Remote Management; MIME Multipart Media Encapsulation; Mobile IP; Mobile IPv6; MMS Message Encapsulation; Mount Service; PPP Multilink Protocol; RFC 2250 MPEG1; MultiProtocol Label Switching Header; Multiprotocol Label Switching Echo; PPP MPLS Control Protocol; WebSphere MQ; WebSphere MQ Programmable Command Formats; Multicast Router DIScovery protocol; Multicast Source Discovery Protocol; MSNIP: Multicast Source Notification of Interest Protocol; MSN Messenger Service; MS Proxy Protocol; Message Transfer Part Level 2; Message Transfer Part Level 3; Message Transfer Part Level 3 Management; MySQL Protocol

N

NetBIOS Datagram Service; NetBIOS over IPX; NetBIOS Name Service; Name Binding Protocol; NetBIOS Session Service; NetWare Core Protocol; Network Data Management Protocol; Novell Distributed Print System; NetBIOS; Microsoft Windows Logon Protocol; Network File System; NFSACL; NFSAUTH; NIS+; NIS+ Callback; Network Lock Manager Protocol; NetWare Link Services Protocol; Novell Modular Authentication Service; Name Management Protocol over IPX; Network News Transfer Protocol; NSPI; NTLM Secure Service Provider; Network Time Protocol; Null/Loopback; NetWare Serialization Protocol; Niksun ATM over T1; Niksun Frame Relay over T1; Niksun PPP over T1; Niksun Bay PPP over T1; Niksun Cisco HDLC over T1

O

ATM OAM AAL; Optimized Link State Routing Protocol; PPP OSI Control Protocol; Open Shortest Path First; DCOM OXID Resolver; [P] PPP Password Authentication Protocol; Packet Cable Lawful Intercept; PC NFS; Packed Encoding Rules (ASN.1 X.691); OpenBSD Packet Filter log file; OpenBSD Packet Filter log file; pre 3.4; Pragmatic General Multicast; Protocol Independent Multicast; SMB Pipe Protocol; Post Office Protocol; Portmap; POSTGRESQL; Point-to-Point Protocol; PPP Multiplexing; PPPMux Control Protocol; PPP-over-Ethernet Discovery; PPP-over-Ethernet Session; Point-to-Point Tunnelling Protocol; ISO 8823 OSI Presentation Protocol; Prism; Precision Time Protocol (IEEE1588)

Q

Q.2931; Q.931; Q.933; Qualified Logical Link Control; Quake Network Protocol; Quake II Network Protocol; Quake III Arena Network Protocol; QuakeWorld Network Protocol

R

IEEE 802.11 Radiotap Capture header; Radius Protocol; Radio Access Network Application Part; Raw packet data; Session Initiation Protocol (SIP as raw text); DCE/RPC Directory Acl Interface ; RDM; DCOM Remote Activation; AFS (4.0) Replication Server call declarations; Routing Information Protocol; RIPng; Redundant Link Management Protocol; Rlogin Protocol; Remote Management Control Protocol; Java RMI; HP Remote Maintenance Protocol; Remote Override interface; Remote Procedure Call; RPC Browser; Microsoft Network Logon; Remote Program Load; Privilege Server operations; Remote Quota; DCE/RPC RS_ACCT; Registry Server Attributes Manipulation Interface; DCE/RPC Registry Server Attributes Schema; DCE/RPC RS_BIND; DCE/RPC RS_MISC; DCE Name Service; RS Interface properties; DCE/RPC RS_PROP_ACCT ; DCE/RPC Registry server propagation interface - ACLs. ; DCE/RPC Prop Attr; DCE/RPC Registry

server propagation interface - PGO items; DCE/RPC Registry server propagation interface - properties and policies; DCE/RPC Registry Password Management ; Registry server administration operations.; DCE/RPC Repserver Calls; DCE/RPC Operations between registry server replicas; DCE/RPC RS_UNIX; Remote sec login preauth interface.; Remote Shell; RSTAT; Resource ReserVation Protocol (RSVP); RSYNC File Synchroniser; RTcfg; Real-time Transport Control Protocol; Routing Table Maintenance Protocol; RTNET; Real-Time Transport Protocol; RFC 2833 RTP Event; Real-Time Publish-Subscribe Wire Protocol; Real Time Streaming Protocol; Reliable UDP; Remote Wall protocol; RX Protocol

S

SADMIND; Microsoft Security Account Manager; Session Announcement Protocol; Fibre Channel Single Byte Command; Signalling Connection Control Part; Signalling Connection Control Part Management; SCSI; Stream Control Transmission Protocol; Synchronous Data Link Control (SDLC); Session Description Protocol; SEBEK - Kernel Data Capture; DCE Security ID Mapper; Java Serialization; ISO 8327-1 OSI Session Protocol; InMon sFlow; SGI Mount Service; Short Frame; Session Initiation Protocol; Sipfrag; Skinny Client Control Protocol; Cisco SLARP; SliMP3 Communication Protocol; Linux cooked-mode capture; SoulSeek Protocol; Cisco Session Management; SMB (Server Message Block Protocol); Short Message Peer to Peer; Simple Mail Transfer Protocol; SNMP Multiplex Protocol; Systems Network Architecture; Systems Network Architecture XID; SNA-over-Ethernet; Subnetwork Dependent Convergence Protocol; Simple Network Management Protocol; Socks Protocol; Nortel SONMP; Spnego; SPNEGO-KRB5; Microsoft Spool Subsystem; SPRAY; Sequenced Packet eXchange; Service Location Protocol; Microsoft Server Service; SSCOP; SSH Protocol; Secure Socket Layer; Network Status Monitor Protocol; Network Status Monitor CallBack Protocol; Spanning Tree Protocol; Simple Traversal of UDP Through NAT; SS7 SCCP-User Adaptation Layer; Microsoft Service Control; Fibre Channel SW_ILS; Symantec Enterprise Firewall; Syslog message

T

T38; TACACS; TACACS+; Microsoft Telephony API Service; Transaction Capabilities Application Part; Transmission Control Protocol; Tabular Data Stream; TEI Management Procedure; Channel D (LAPD); Telnet; TEREDO Tunnelling IPv6 over UDP through NATs; Trivial File Transfer Protocol; Time Protocol; DCE/RPC TokenServer Calls; Transparent Network Substrate Protocol; Alteon - Transparent Proxy Cache Protocol; TPKT; Token-Ring; Microsoft Distributed Link Tracking Server Service; Token-Ring Media Access Control; Time Synchronization Protocol; Tiny Transport Protocol; BEA Tuxedo; Tazmen Sniffer Protocol

U

DCE/RPC FLDB UBIK TRANSFER; DCE/RPC FLDB UBIKVOTE; Universal Computer Protocol; User Datagram Protocol; UDP Encapsulation of IPsec Packets; Unreassembled Fragmented Packet

V

Async data over ISDN (V.120); V5.2-User Adaptation Layer; Banyan Vines ARP; Banyan Vines Echo; Banyan Vines Fragmentation Protocol; Banyan Vines ICP; Banyan Vines IP; Banyan Vines IPC; Banyan Vines LLC; Banyan Vines RTP; Banyan Vines SPP; PPP VJ Compression; 802.1q Virtual LAN; Virtual Router Redundancy Protocol; Virtual Trunking Protocol

W

WAP Session Initiation Request; WAP Binary XML; Web Cache Coordination Protocol; Wellfleet Compression; Wellfleet HDLC; Who; Microsoft Registry; Microsoft Workstation Service; IEEE 802.11 wireless LAN; IEEE 802.11 wireless LAN management frame; AVS WLAN Capture header; Wireless Session Protocol; Wireless Transport Layer Security; Wireless Transaction Protocol

X

X.25; X.29; X11; X Display Manager Control Protocol; X.25 over TCP; Xyplex

Y

Yahoo Messenger Protocol; Yahoo YMSG Messenger Protocol; Yellow Pages Bind; Yellow Pages Passwd; Yellow Pages Service; Yellow Pages Transfer

Z

Zebra Protocol; Zone Information Protocol

2. Voice over IP (VoIP) Protocols

H.323 v 4 - H.225, H.245, Q.931; RTP, RTCP, SCCP, SIP, MGCP (IPDC/SGCP)

Codecs Supported: G. 711, G.723 & G.729*

* Playback not supported

3. Application Reconstruction

Supported Protocols

The following protocols are supported for Application Reconstruction:

- SMTP
- POP3
- IMAP4
- HTTP
- HTTPS
- FTP
- MSNP
- YMSG
- OSCAR
- SSL3

To view application data for other TCP application protocols (e.g., TELNET) you can use ASCII or HEX options.

Application Reconstruction

Handling missing packets has been implemented; however, an application may be reconstructed partially due to missing packets. You can view packets using ASCII or HEX options.

The appliance reconstructs SMTP, POP3, IMAP4, HTTP, and HTTPS sessions.

The current version of application reconstruction complies with the following RFCs:

- RFC 821 – SMTP
- RFC 1945 – HTTP/1.0
- RFC 2068 – HTTP/1.1
- RFC 1869 – SMTP service extensions
- RFC 1939 – POP3
- RFC 2060 – IMAP4
- RFC 822 – Standards for the format of ARPA internet text messages
- RFC 1341 – MIME
- RFC 959 – File Transfer Protocol
- RFC 2428 – FTP Extensions for IPv6 and NATs
- RFC 2246 – TLS 1.0

A Email Reconstruction

Email session reconstruction will reconstruct the following data from the stored packets:

- Date
- To/from email IDs
- cc e-mail IDs
- Subject
- Message body
- Attachments

The attachments, if encoded, are constructed only if the attachment is base64, quotable printable, 7-bit, or 8-bit encoded. Only RFC 1341-based MIME attachments are reconstructed.

B HTTP Reconstruction

Web reconstruction rebuilds the Web page and the embedded objects, if available. Embedded objects will not be available if they were locally cached and not transmitted as part of the browsing session. Web reconstruction can recreate the complete web page as the original browser rendered it, even when embedded objects are sent across multiple sessions. If encoded, embedded objects are reconstructed if they are base64, quotable printable, 7-bit, or 8-bit encoded. Only RFC 1341-based embedded objects are constructed.

C Reconstruction Details

The details pane displays a list of sessions for the selected host or application (or all the sessions). The selection of applications is performed via tabs described below:

Tab	Description
Applications	<p>The Applications screen displays 'reconstructable' sessions (application, web page, chat, email, ftp, or telnet) only.</p> <p>The screen displays the following session details:</p> <ul style="list-style-type: none"> - ID: The session ID. - Start Timestamp: The start date/time for the session. - Client IP: The client's IP address. - Server IP: The server's IP address. - Summary: Displays a summary of the session. For example, URL of a web page. The icons in the column indicate the application type - web page, email, FTP or chat.
Web Pages	<p>Displays web sessions. The screen displays the session ID, Start Timestamp, Client IP, and Server IP and URL of web sessions. The supported file formats are .html, .jsp, .jpg, .gif, .js, etc.,. You can reconstruct HTTP and HTTPS sessions.</p>
Emails	<p>Displays email sessions. The screen displays session ID, Start Timestamp, Client IP, and Server IP, the email addresses (sender and receiver), subject and attachment file names.</p>
FTP	<p>Displays FTP sessions. The screen displays session ID, Start Timestamp, Client IP, and Server IP, the FTP user name and files transferred during the session.</p>
Chats	<p>Displays chat sessions. The screen displays the Session ID, Start Time, Client IP, Server IP and Buddy List of the IM sessions. You can reconstruct peer-to-peer instant messaging (IM) sessions via MSN Messenger (port 1863), Yahoo (port 5050) and AOL Instant Messenger (port 5190).</p>
	<p>Note: It is possible that the IM traffic might use some other port, for example, when connected through the proxy server; the default port may not be used.</p>
Telnet	<p>Displays telnet sessions.</p>
Sessions	<p>The Session screen displays details of all the sessions for the selected interface. The screen displays the following information:</p> <ul style="list-style-type: none"> - ID: Session ID. - Start Timestamp: Start date/time for the session. - End Timestamp: End date/time for the session. - Client IP: Client's IP address. - Client Port: Client's port number and, if applicable, the application name. - Client Data: Data sent by the client in bytes. - Server IP: Server's IP address. - Server Port: Server's port number and, if applicable, the application name. - Server Data: Data sent by the server in bytes.

D Reconstruction Options

Options	Description
Auto View	Based on the data, the best presentation option is automatically selected.
ASCII	<p>The default presentation format is auto view.</p> <p>ASCII view of the selected information (server, client, or both). Blue and red indicate server and client information respectively.</p> <p>The ASCII view displays a decrypted ASCII dump of the transferred application data. In addition, the following SSL fields are also displayed:</p> <ul style="list-style-type: none"> - Session id - Key Exchange Algorithm - Cipher Suits - Certificate - Server and Client Random - Server and Client MAC - Server and Client write key - Md5_hash, sha_hash - Alert Messages
HEX	HEX and ASCII view of the information translated into a readable format; the output refers to the selected option (server, client, or both). The hex view displays a hex dump of decrypted SSL data.
EBCDIC	Presents data in EBCDIC format.
Encode	Displays encoded data.
Email Viewer	Displays the reconstructed session in email format.
Web Page Viewer	Displays the reconstructed session in web page format.
FTP Viewer	Displays the reconstructed session in FTP format.
IM Viewer	Displays a reconstructed chat session.
Packet Viewer	Opens the packet viewer screen.
Archive Data	The selected data is archived. The archived dataset can be accessed from the Traffic Analysis screen.
Save File	<p>A 'File Download' dialog box opens that allows you to specify the path and name for the downloaded data file.</p> <p>The raw packet data is dumped in the ASCII format.</p>

Note: Sessions that cannot be reconstructed are displayed in ASCII format.

4. Available Recording Network Interfaces

- Ethernet (10/100 Mbit/s)
- Ethernet (10/100/1000 Mbit/s, copper / fiber)
- T1/E1 (channelized/clear, 1,5/2 Mbit/s)
- T3/E3 (clear, 44,7/34 Mbit/s)
- V.35 (34 kbit/s)
- X.21 (64 kbit/s)
- HSSI (High Speed Serial, >34 Mbit/s)
- FDDI (Fiber Distributed Data Interface 100Mbit/s)
- PoS (OC-3/STM-1, 155 Mbit/s)
- PoS (OC-12/STM-4, 622 Mbit/s)
- ATM over DS3 (44,7 Mbit/s)
- ATM (OC-3/STM-1, 155 Mbit/s)
- ATM (OC-12/STM-4, 622 Mbit/s)

Remark: Fiber Interfaces available as Single and Multimode Fiber



If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80

Fax: +49-89-24 20 91 81

le

le