



FOXREPLAY ANALYST

REAL-TIME STREAMING INTERCEPTION ANALYSIS TECHNOLOGY

THE ACTUAL WIRETAPPING OF INTERNET COMMUNICATIONS IS ONLY THE FIRST STEP IN MAKING MAXIMUM USE OF INTERCEPTED INFORMATION. ON TODAY'S BROADBAND INTERNET A LARGE SET OF PROTOCOLS IS USED. COMBINED WITH INCREASED AWARENESS OF INTERCEPTION, THIS MEANS THAT AGENCIES THAT WANT TO GAIN INSIGHT INTO INTERNET TRAFFIC NEED THE BEST ANALYSIS SOFTWARE AVAILABLE.

USE AND WORKFLOW

FoxReplay Analyst interprets intercepted internet, and reconstructs all communications so they can be viewed as easily as the internet itself. Besides reconstruction, communications are played back in the original order and appearance, guaranteeing your ability to "see what your target saw" - and more.

Multiple analysts, multiple streams of interception, connected seamlessly. Communications are available in chronological order, for each analyst the system stores which pages have been viewed already, and how much work remains. Additionally, employees can notify each other of interesting pages, or annotate relevant intercepts with comments. Statistical information provides managers with insight into the percentage of intercepted communications viewed and analysed. Finally, administrators can configure access rights for each user and each interception stream, while sign-on optionally integrates with your pre-existing authentication solution. FoxReplay Analyst goes beyond simply viewing intercepted Internet, but forms a complete work-flow solution allowing organizations to turn intercepted packets into rock-solid evidence.

REALTIME & STREAMING TECHNOLOGY

Internet conversations can last many hours, and some protocols use connections that persist for days at a time. As the internet is real-time and live, FoxReplay Analyst starts displaying data from the first intercepted packet. This is possible because unlike traditional systems, FoxReplay Analyst does not process traffic in sizeable batches, but does so on a per packet basis. Our streamlined data transport enables the interpretation of content within seconds of its interception.

SUPPORTED PROTOCOLS

All plaintext protocols in general use are supported. Of specific note is our full support of IPv6 protocols, both native and tunnelled, including all protocols running on top of IPv6. Additionally, rapid updates mean all new features of modern chat programs are supported soon after their introduction. This includes the potentially relevant 'avatar images', wallpapers and other non-verbal communication methods used in for example the Microsoft Messenger. Naturally FoxReplay Analyst offers full support for voice over IP, whether standalone or as part of an existing chat protocol.



SIGNALS INTELLIGENCE

SIGINT applications have special needs due to the irregular collection of signals, and the resulting massive amounts of data. FoxReplay Analyst has support for these special needs, and can be tailored to your specific situation. Contact us for further details.

MODULAR, FLEXIBLE

Interception is never standard, and the modular and flexible design of FoxReplay Analyst reflects this. Intercepted packets can easily be streamed into the core program, from a variety of sources, including all industry standard transmission protocols (ETSI, TIIT, J-STD) and files (PCAP, TIIT). Additionally, new protocols can be added and existing ones updated, on the fly, without any downtime.

Organizations typically have authentication structures in place, for example using Active Directory, LDAP or Radius, FoxReplay Analyst can be customised to integrate with your pre-existing authentication systems.

SCALABILITY

As average internet bandwidths increase, together with the time spent online, data processing needs continue to grow at double digit rates. FoxReplay Analyst is inherently scaleable, both in number of servers as in number of processors. Our powerful scalability technologies enable us to utilize the power of many servers on a single interception stream, or divide servers over a number of separate interception streams. Addition of extra servers is flexible and can occur during full streaming operation, without downtime.

“I18N” - INTERNATIONALISATION

Because of faithful reconstruction of the original content, all native tools are available to display intercepted communications in its authentic form and script. This means that all script types supported by the internet are available for analysis.

DEEP CONTENT SEARCH

Information can be hidden deeply within communications - for example in a Word document, embedded in a ZIP file, transmitted over MSN which in turn is transported over an HTTP proxy. FoxReplay Analyst unpeels these layers and makes their contents available for viewing, and more importantly, searching. Deep Content Search allows operators to access information that would otherwise remain hidden, vital in a world where increasing flows of data make it ever harder to discern important clues.

FILTERING

To filter out irrelevant data, and show relevant content, FoxReplay Analyst comes with advanced filtering capabilities, which allow users to tailor which data is displayed. Additionally, system administrators and advanced users can create more powerful rules that match whole classes of traffic found not to be relevant, like for example, Windows Update downloads. For email, FoxReplay Analyst technology makes it possible to filter out spam, and classify large streams of email into separate categories.

TRAINING, INSTALLATION, INTEGRATION, CUSTOMISATION

While FoxReplay Analyst is very easy to use, system administrators, engineers and IT specialists will benefit from our in-depth knowledge and profit from our best practices guidelines. Furthermore, course material for case-workers is available, suitable for in-house training. Although FoxReplay Analyst is available as a separate boxed product, FOX-IT is pleased to provide installation, integration and customisation services to make our product tailor-made to your unique needs and network.

BENEFITS OF FOXREPLAY ANALYST

	FOXREPLAY ANALYST	TYPICAL COMPETITON
Real-time	Yes	No, typical delay of hours
Streaming	Yes	No, batch processes
Full-text Search	Yes	No
Rapid protocol updates	Two weeks	Annually
Custom protocols	Yes	Difficult
As easy as the internet	Yes	No
“See what the target saw”	Yes	No
Simultaneous Communications side by side	Yes	No
All languages	Yes	No
Client-side software	Web browser plugin	Additional applications

