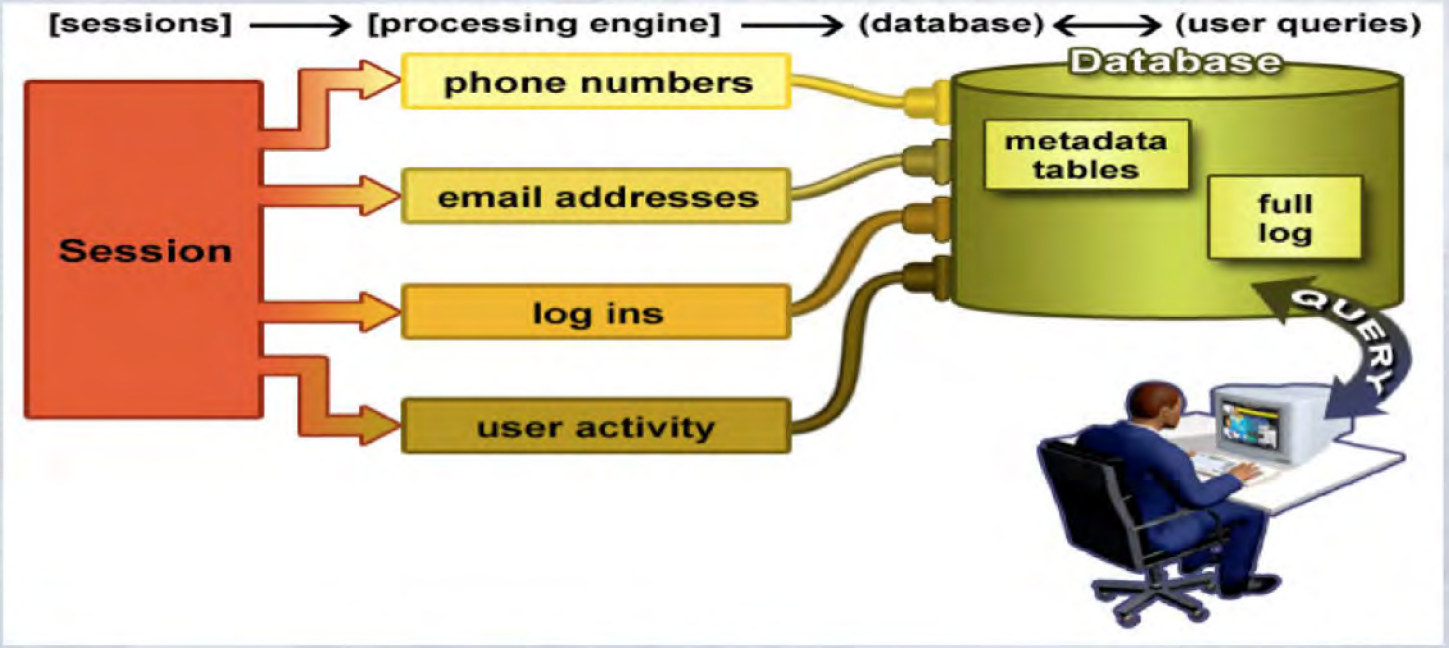
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

What XKS does with the Sessions

Plug-ins extract and index metadata into tables



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Plug-ins

Plug-in	DESCRIPTION
E-mail Addresses	Indexes every E-mail address seen in a session by both username and domain
Extracted Files	Indexes every file seen in a session by both filename and extension
Full Log	Indexes every DNI session collected. Data is indexed by the standard N-tupple (IP, Port, Casenotation etc.)
HTTP Parser	Indexes the client-side HTTP traffic (examples to follow)
Phone Number	Indexes every phone number seen in a session (e.g. address book entries or signature block)
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc.

TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

Examples of "advanced" Plug-ins

Plug-in	DESCRIPTION
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc. (AppProc does the exploitation)
Document meta-data	Extracts embedded properties of Microsoft Office and Adobe PDF files, such as Author, Organization, date created etc.