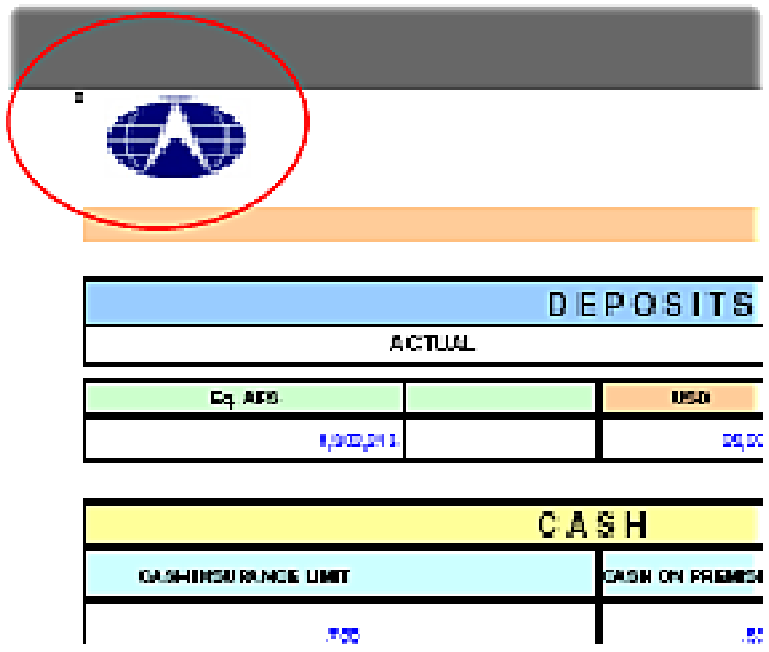
[redacted]

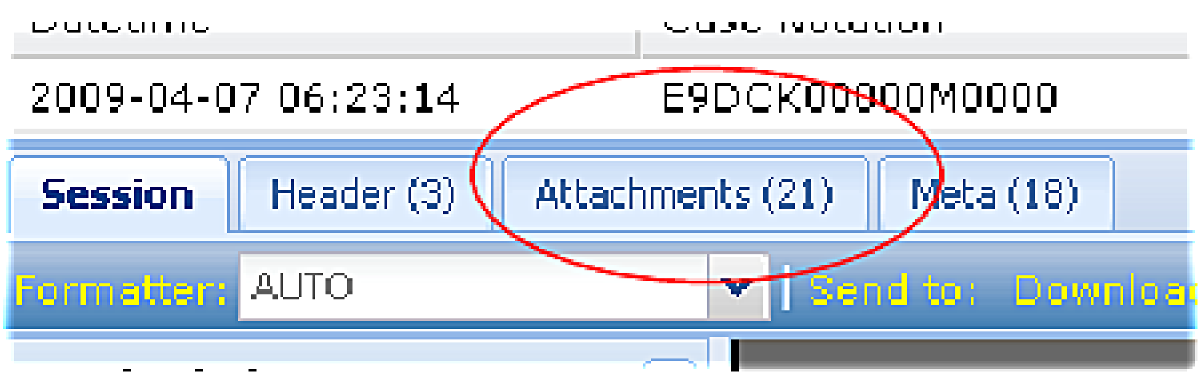
Booz | Allen | Hamilton
ADET – E92

Using XKS to find and search for logos embedded in documents

XKEYSCORE will parse out the logos inside of documents like MS Office and Outlook emails. If you're traffic hasn't aged of, load it into a session viewer and hopefully you'll see where there's a logo or attachment. See here, this spreadsheet has a logo in it.

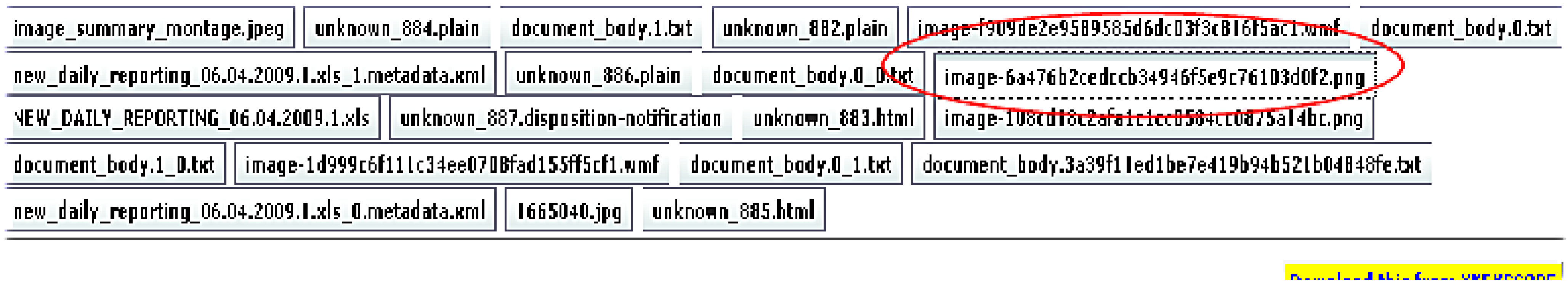


(TS//SI//REL) XKEYSCORE takes that logo and calls it an attachment. Click on Attachments to see all of the attachments.



2009-04-07 06:23:14 E9DCK00000M0000

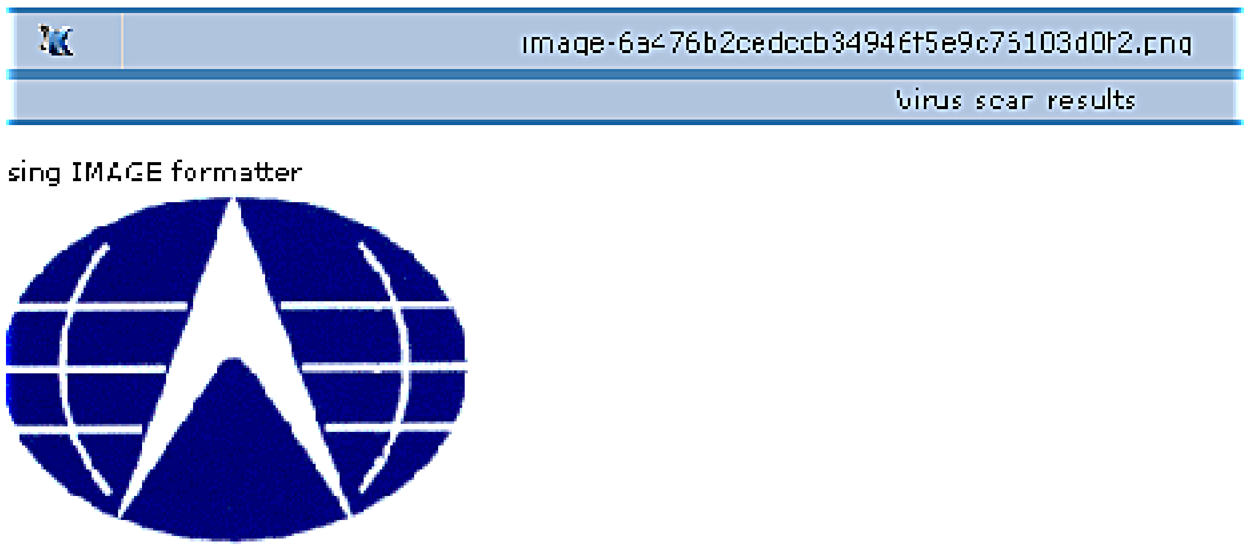
(U//FOUO) In the Attachments window, look for ones with jpg or png.



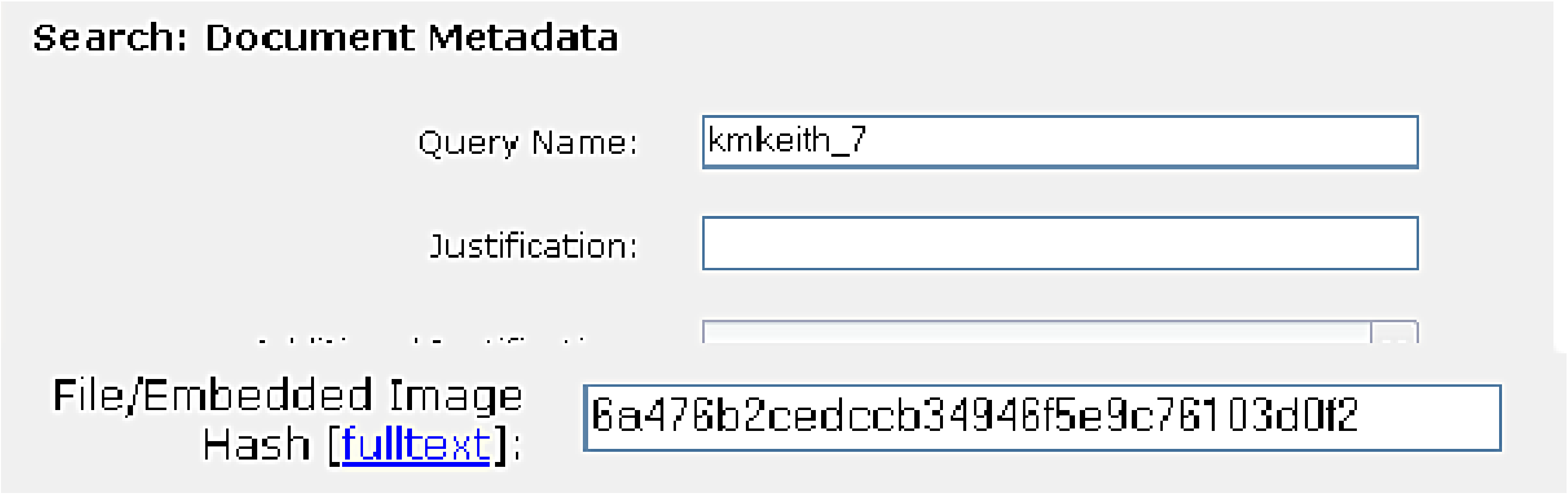
image_summary_montage.jpeg | unknown_884.plain | document_body.1.txt | unknown_882.plain | image-f909de2e9589585d6dc03f3c816f5ac1.wmf | document_body.0.txt
new_daily_reporting_06.04.2009.1.xls_1.metadata.xml | unknown_886.plain | document_body.0_0.txt | image-6a476b2cedccb34946f5e9c76103d0f2.png
NEW_DAILY_REPORTING_06.04.2009.1.xls | unknown_887.disposition-notification | unknown_883.html | image-108cd18c2afa1c1cc0584cc0875a14bc.png
document_body.1_0.txt | image-1d999c6f111c34ee0708fad155ff5cf1.wmf | document_body.0_1.txt | document_body.3a39f11ed1be7e419b94b521b04848fe.txt
new_daily_reporting_06.04.2009.1.xls_0.metadata.xml | 1665040.jpg | unknown_885.html

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20340401

(U//FOUO) Notice the hash of the jpg



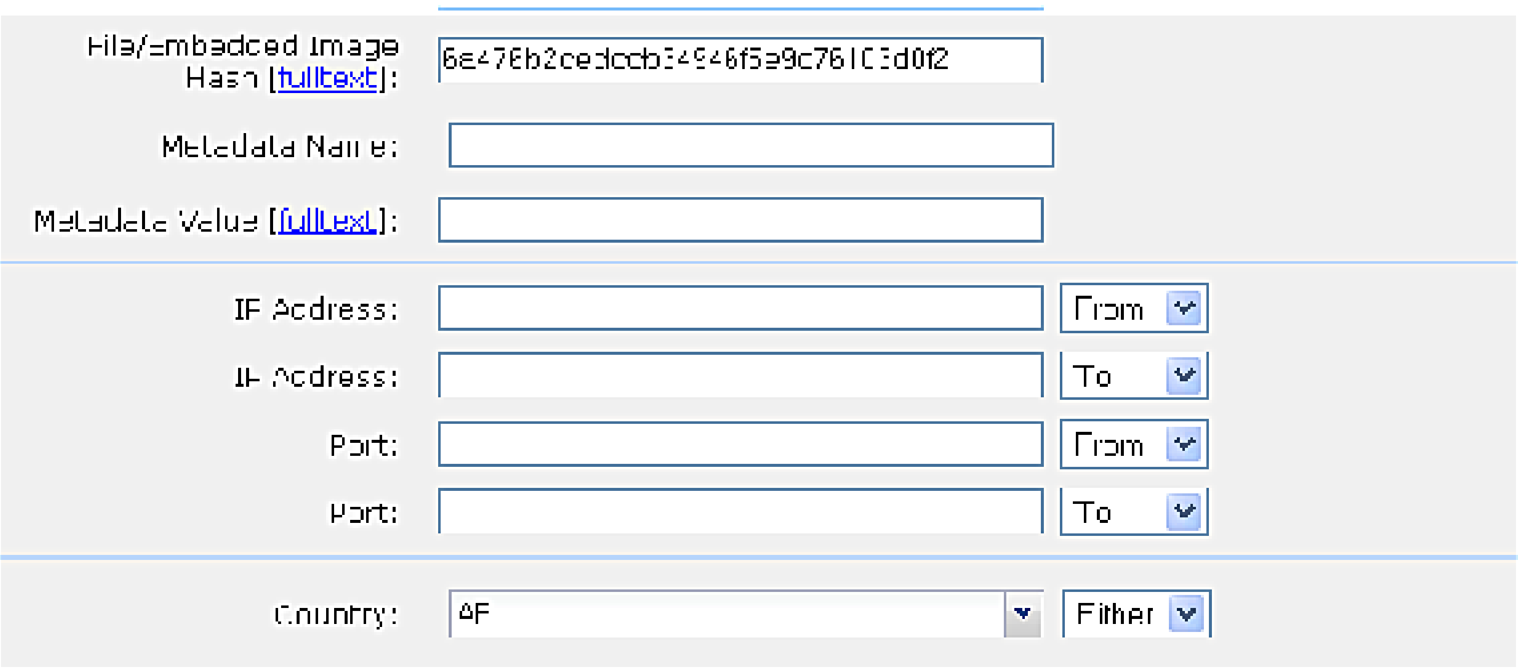
(TS//SI//REL) Now you take the 32-character hash (e.g. *6a476b2cedccb34946f5e9c76103d0f2*) and paste that into a Document Metadata search under the File/Embedded Image Hash field:



Search: Document Metadata

Query Name:	kmkeith_7
Justification:	
File/Embedded Image Hash [fulltext]:	6a476b2cedccb34946f5e9c76103d0f2

(TS//SI//REL) Before you hit submit, you MUST think if the logo could be used by 5-EYES protected entities. It should go without saying, but take extra precaution if you think it could bring back 5-EYES traffic. What would you do to ensure it's foreign? Maybe AND that with a country?



File/Embedded Image Hash [fulltext]:	6a476b2cedccb34946f5e9c76103d0f2	
Metadata Name:		
Metadata Value [fulltext]:		
IP Address:		From
IP Address:		To
Port:		From
Port:		To
Country:	AF	Either

(TS//SI//REL) Then hit submit and check your results. Your results MAY show you actual files that were sent to and from people you've never HEARD OF (how cool is that?)

Happy hunting.. [redacted]