Data Generation Scenario Build-Out Guidelines

Data Set was created by students at Marshall University

**Scenario:**

In a jurisdiction where Owls are illegal to trade and buy, two users are discussing the illegal trade of owls. The computer and mobile device that will be taken into evidence are of a user who is attempting to purchase owls illegally. The user contacts another user who can provide an owl in exchange for cash. An owl is decided upon, and an exchange is scheduled. After the exchange, a communication message is sent confirming the owl purchase has been completed.

Please ensure you populate the computer with distractor data. There should be images of owls and of other animals that are not owls. Include normal noise distractor data as well. Evidence of the intent should be on the phone. Confirmation of the sale should be made from the PC.

It is important that the case require looking at both the PC and the phone to be able to confirm all of the details of the transaction. Meeting location, type, cost, discussed on phone. Confirmation of purchase and email with attachments on Computer only.

**Evidence**

* PC Image with Windows 10
* Full/Physical image of Nexus 5 Android 6.0 Mobile Phone

Below is a list of the Guidance that was given, please see the log documents for actual data that was populated.

**Android device**

* + Search engine:
    - Use a search engine to search for images of Owls
    - Use multiple search engines
  + SMS:
    - Create SMS messages (only with other test devices – do not use real people)
    - One message sent via SMS should confirm the time of the trade (other details will be discussed in Music.ly
  + Chat Client
    - These apps should be protected with CM Security AppLock (download and protect this app before using)
    - Use Music.ly to have chat conversations with the Owl trader regarding meeting location and type and cost. Also discuss that you will send pictures of the image via email. The owl trader should share his email address here.
    - Have conversation with the owl trader on Skype, but do not discuss the trade here!
    - Create unrelated content in this app
  + Images
    - Download pictures of owls. Download other images of birds/foul that are not owls as distractor data.
  + Social Networks
    - Use for creation of noise data (Instagram, twitter, facebook)
  + Map
    - Map the route to the rendez-vous point for the owl purchase
  + BEFORE IMAGING - On the date the image is made of the mobile device – before imaging enter an INCORRECT pincode so that the applock password (with the camera covered with a post it) so that an “intruder selfie” is made.

**PC**

* + Web searches
    - Conservation of Owls
    - Endangered species lists
    - Different types of owls and their windspans
  + Shopping searches
    - Look to purchase owls on several ecommerce sites (ie Amazon, Etsy)
  + Chat Clients
    - Have conversations on Skype, but NOT with the Owl Trader
    - Use Pidgin to talk with the Owl Trader, but do not discuss the transaction EXCEPT the confirmation at the very end that the transaction has taken place.
  + E-mail
    - Gmail - Send email with picture attachments depicting the type of owl you are interested in purchasing across email form the computer.
  + Documents
    - Download some documents (.pdf, .txt, .xls) of both owl and noise data. Save ones with owl content to the desktop, but then relocate that document elsewhere on the filesystem.
  + Social Networks
    - Noise data (Instagram, twitter, facebook)
  + OS artifacts
    - LNK Files
      * Open multiple files from local and external (USB) drives including some of the files with owl content that you download
    - Recycle Bin
      * Move some items to the recycle bin, but do not empty
    - Shellbags
      * View scenario based images from a folder location (of your choosing) set to “Extra Large Icons”

**Keywords for conversations, searches, and chats**

* + Owl
  + Owlet
  + Feathers
  + Eggs
  + Crossbreeding
  + Nocturnal
  + Nest
  + Hoot
  + Conservation
  + Wingspan