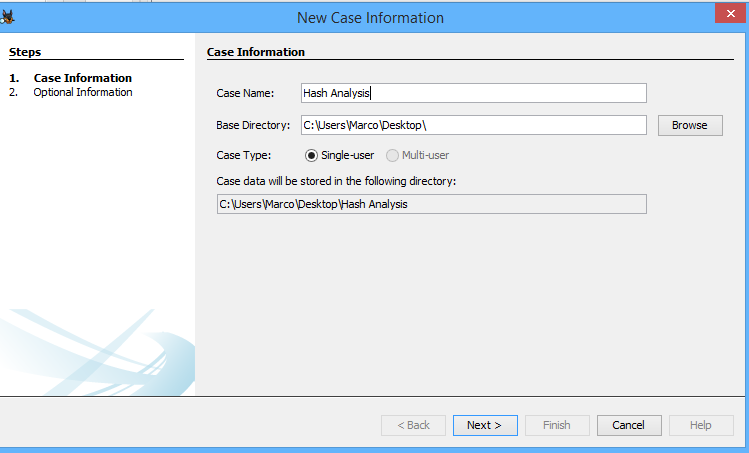
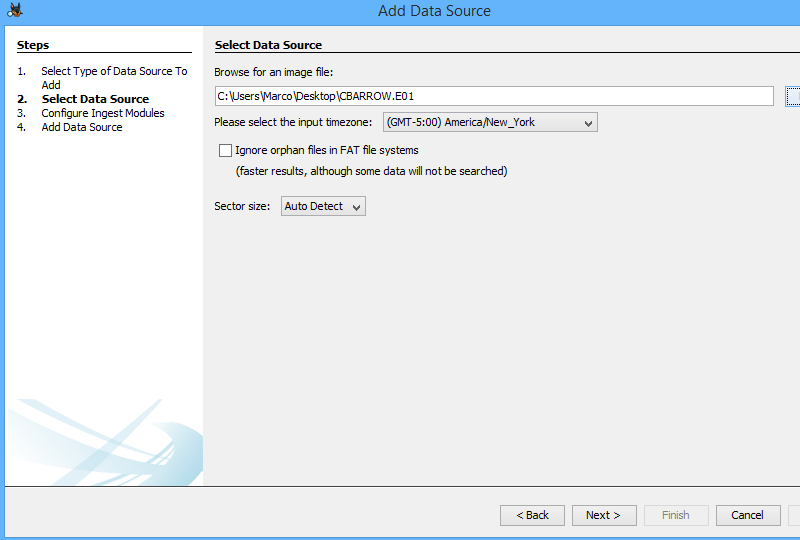
By: Jason Lu and Marco Seman

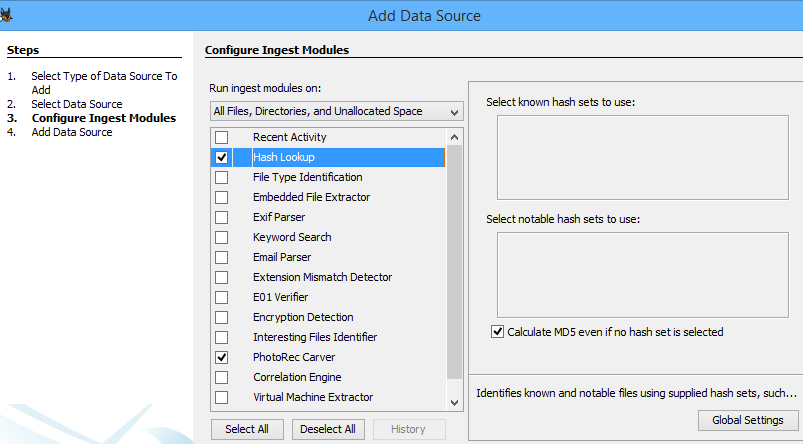
1. Launch Autopsy and create a case, Create New Case and name it as “Hash Analysis”.



2. Add data source type: choose Disk Image; browse and select the path to "CBARROW.E01".

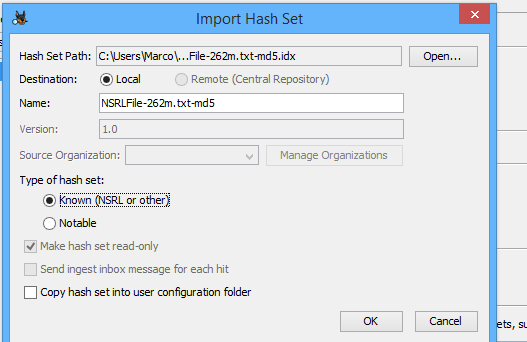


3. In the Ingest (processing) modules window, uncheck all modules except the “Hash Database Lookup Module” and “PhotoRec Carver Module”;

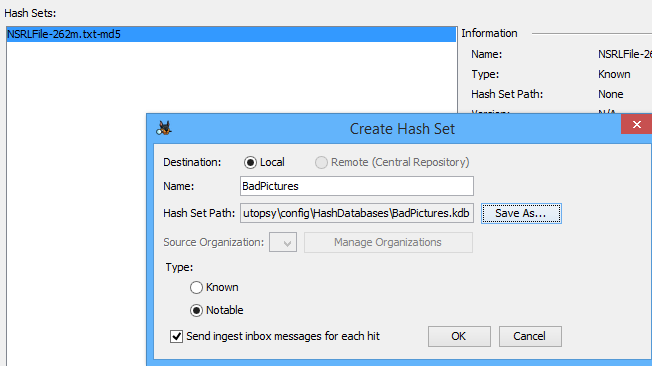


4. Click “Hash Database Lookup Module” and the click Global Setting.

5. At the “Global Hash Lookup Setting” window, click “Import Hash Set”, open your downloaded NRSL hash set index file (.idx), and check the “Known” option under the Type of Hash Set.



6. Click “New Hash Set” and then input “BadPictures” in the name field and choose a “Hash Set Path”, and, and check “Notable” type, and check “send ingest inbox messages for each hit”.



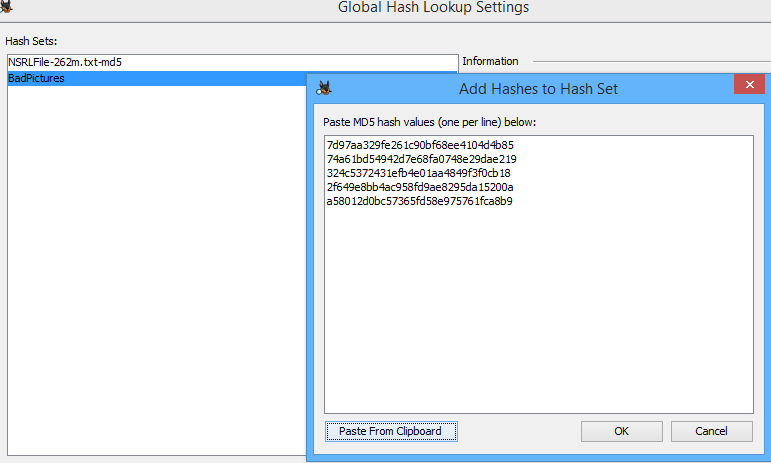
7. Click “OK”; and click “Add Hashes to Hast Set” and then copy and paste the following MD5 hashes

7d97aa329fe261c90bf68ee4104d4b85

74a61bd54942d7e68fa0748e29dae219

324c5372431efb4e01aa4849f3f0cb18

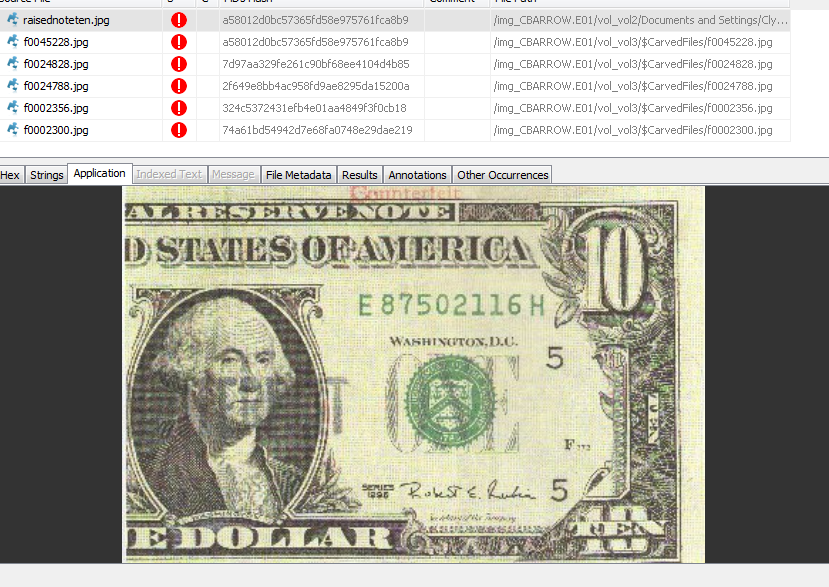
2f649e8bb4ac958fd9ae8295da15200a



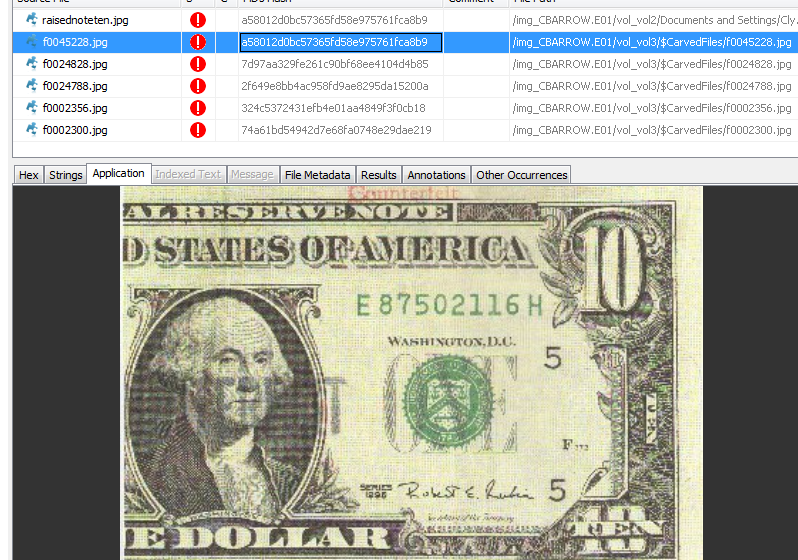
9. Review the search results under Results > Hashset Hits > BadPictures, and find all the hits.

There are six total bad hits

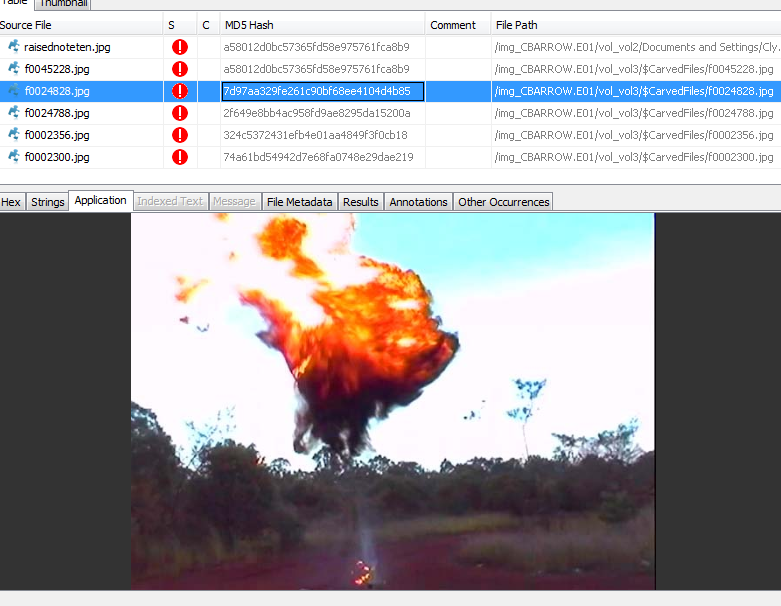
The First bad picture: raisednoteten.jpg



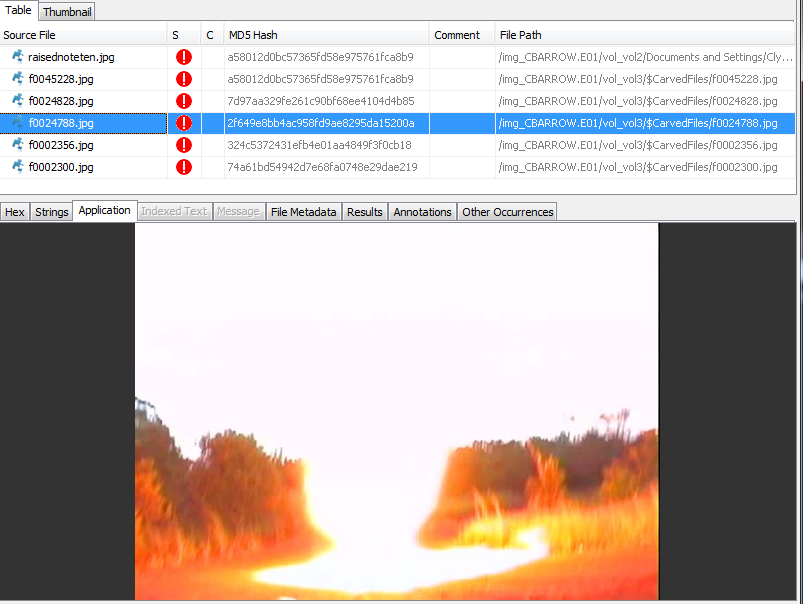
Second:f0045228.jpg



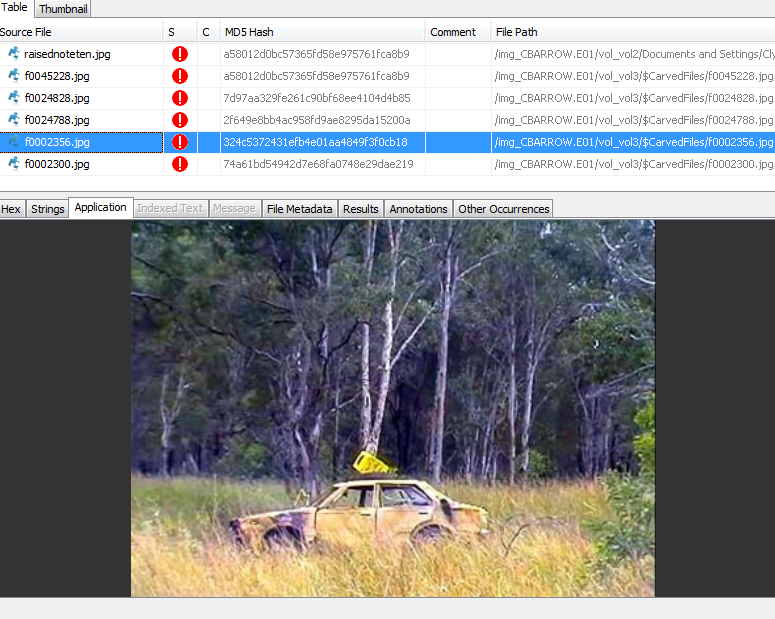
Third: f0024828.jpg



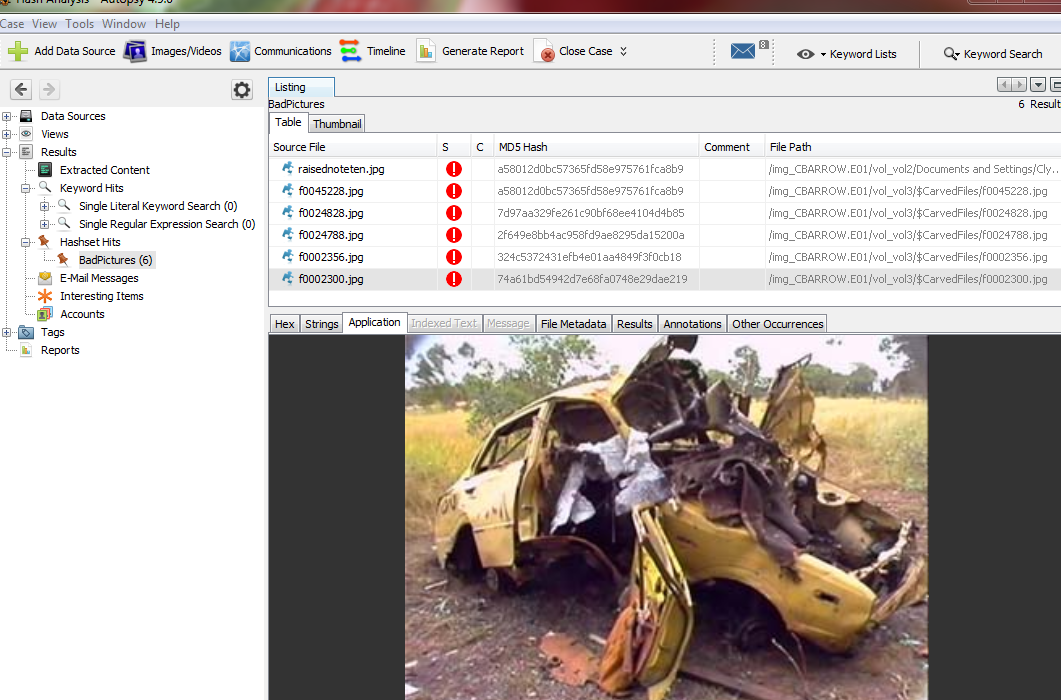
Fourth: f0024788.jpg



Fifth: f0002356.jpg

****

Sixth: f0002300.jpg

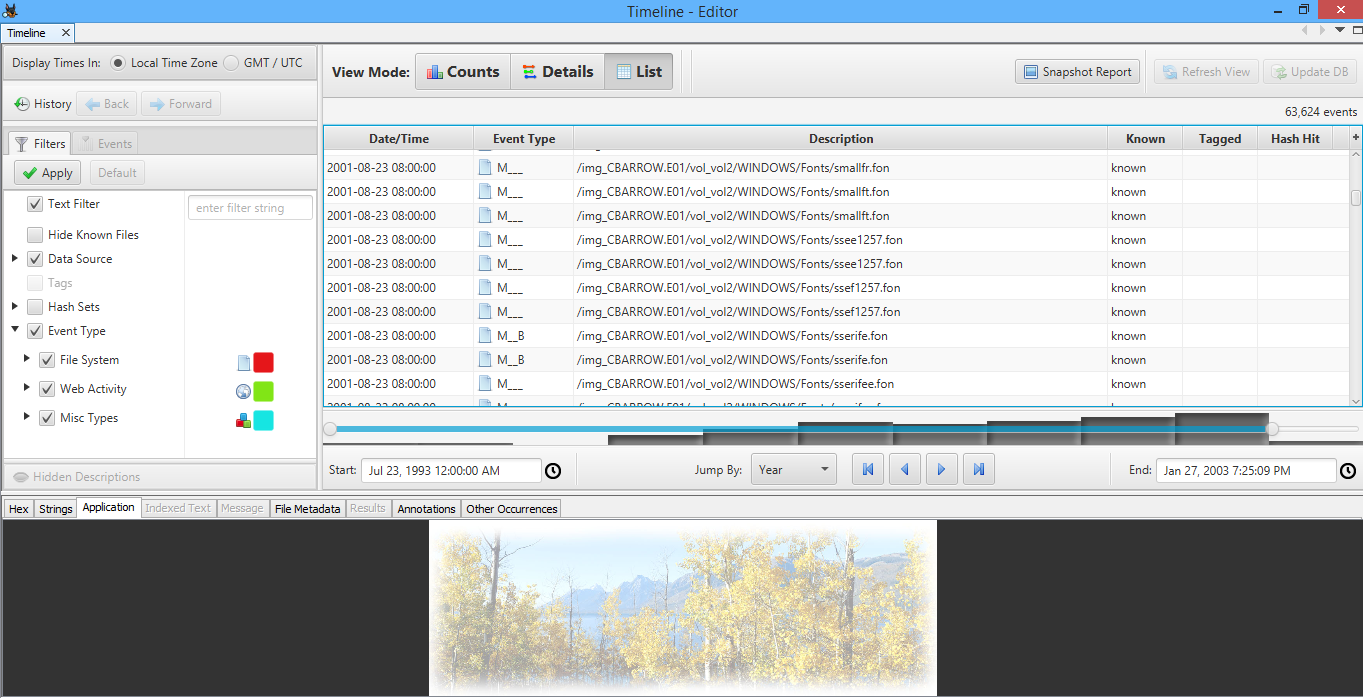


After reviewing some know files, there’s a small percentage that contains bad pictures. File extension such as.GIF, PSD has the greatest percentage that are pictures

10. Click and Open “Timeline” window, select “List” view mode, and review some known files.

Under the timeline view, the known files contains following file extensions:

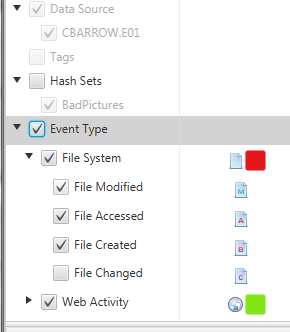
* .txt, .gif, .psd, .dll, .jpg, .acs, .cab, .htm, .icw, .ver, .dun, .exe, .ini, .dat, .icm. .sys. .fon, .inf, .mfl, .mof, .msc, .cat, and much more



What we learned:

For lab 7, we learned how to use the hash database lookup and photoRec carver module to find the contents inside of the cbarrow image. We learned that the hash database lookup is used to calculate the MD5 hash to determine whether the file is known as a bad file. We also learned that the photoRec feature carves files from unallocated spaces in the data source and sends the file found in the ingest processing chain. When searching for bad pictures, we learned that if we place the MD5 hash of the file and add it to the hash set, the software will find the exact location of the file and reveal its data and location.

We also learned some interesting features about the timeline. By using the list view mode, we can view specified file information such as whether the file has been created, modified, accessed, or changed.



We also learned that we can search files by their dates for example, If we want to do an investigation between December 1995 to February 1997, we can use the timeline boundary to target that time period, by doing that we can narrow it down to 7 events during that time period, which it had shortened the time will take for the investigation

