X-Ways Cheat Sheet

- Erik Martin -

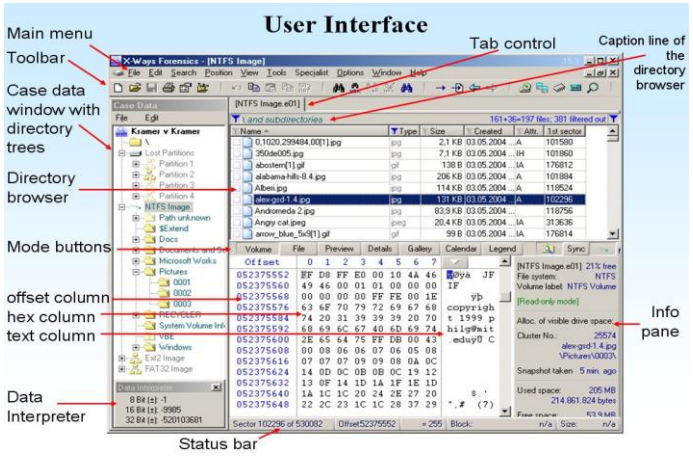
X-Ways Initial Settings

- Initial Settings: Click Options - > General
- Verify the paths for
  - Temporary Files
  - Evidence
  - Cases
- Click into “Display time zone” and verify the desired timezone is selected
- Choose “Notation” to view or change the way Date/ Time is displayed

General X-Ways Rules and Information

- Legend key, located in mode button bars, is used for Icon help
- X-Ways is unable to perform more than one process at a time
  - Example: Unable to both search for an item and extract it at same time
- Some checkmarked boxes have multiple states
- Check marks on boxes to the right of setting options will indicate that a process has already been run
- Tag (or select) items by clicking on the box to the left of their name
  - Will turn purple when tagged
- Timestamp Features:
  - To view timezone info: Click on case - > right click on properties -> see description

User Interface



Creating a Case - Instructions

1) Begin in the Case Data window
2) Click on file
3) Click on create new case
4) Input information
   a. Case title
   b. Directory
   c. Examiner
   d. Most other default values will work
5) Click ok button at bottom of window to create new case

X-Ways Important UI Features

- Column Customization: Ability to filter, resize, and reorder
- Case Processing: Refine Volume Snapshot
- Mode Buttons:
  - Partition: Hex view with partition offset, physical
  - File: Hex view with offset starting at zero, logical
  - Preview: Best guess on how file should look
  - Details: Metadata
  - Gallery: Images
  - Calendar: Shows events in calander form
  - Legend: List of icons and their associated meanings
  - Recursion: Useful when searching entire directory contents
  - Search Hit: Use to check list of all completed search results
  - Events: Similar to Plaso; timelining

Viewing Evidence Information

1) Right click on the image in Case Data Window
2) Click on properties
3) A window will open -> Description will contain information regarding the evidence

Case Processing (Refine Volume Snapshot) - Instructions

1) Begin on top menu bar
2) Click on Specialist
3) Click on the first option, Refine Volume Snapshot

Refine Volume Snapshot (RVS) Information

- Processes case based on settings, including: hashes, emails and signature analysis
- Can run RVS on images and files added to the case
  - When tagging individual files you want, open up RVS, select greedy, and check the tagged items only box
- Additional columns will be populated when run (example: skin tone)
- 3 Levels of Processing:
  1) Disk Image [1]
     - Clicking on Particulaly thorough... will reveal an options box for more customization
     - File header signature search = file carving
  2) Individual Files [2]
     - Threading option (immediate) with max threads
     - To select all options, click on the far-right box (greedy mode)
  3) Searching [3]

Refine Volume Snapshot Processing Options

- Must haves:
  - Particularly thorough file system data structure search [1]
  - File header signature search [1]
  - Compute Hash [2]
  - Verify file types with signatures and algorithm [2]
  - Extract metadata, browser history, and events [2]
  - Include contents of file archives [2]
- Nice to haves:
  - Greedy mode [2]
  - Indexing [2]
  - Match hash values against database [2]

Search (Simultaneous Search) - Instructions

1) Click on Search on the top navigation pane
2) Select simultaneous search
3) Add your search term(s) into the search box
   a. Take a look at the options to better perform your search

Search Options

- Can stop searching if "one hit per file"
- Decode text in file (will search pdfs, email, etc. for search terms)
- Able to understand grep
  - grep:[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3} See regex manual for more info
- For certain check mark boxes
  - Full check = every line is checked
  - Half check = prepend the search term with : (line is case sensitive)
- To see search results, click on the binoculars mode button

Did you know

- X-Ways can image/clone disks
- X-Ways can edit disks
- Defining a block / carving from unallocated
  1) Select group of hex
  2) Right click and select add to block file
  3) Add (or create) to report table
  4) If selected in partition mode: results will show up in path unknown directory
  5) If Selected in file mode: results will show up as child of selected file
- X-ways can refine PSTs
- Able to open MFT, USN and LogFile individually as well as evt, evtx, internet history, ost, and pst to name a few
  - X-Ways will parse each individually
- X-Ways will parse and view the registry, similarly to reg ripper

Filtering – General Information

- To see all filtering options, click CTRL F5
- Filtering is distinguished by the funnel icon
  - Purple funnel – filter is applied
  - Grey funnel – filter is not applied
- Master filter toggle is directly above the column, next to the Case Data pane
  - Left click toggle for master filter
  - Right click will list all filters
- Individual filter toggle is located on each column's title
  - Left clicking the funnel will pop up a window to add filter options
  - Right click toggle column filter
  - Can filter on multiple columns at once
  - Can freeze columns (in filtering options - first scrollable column)

Filtering by Column

1) Left click on the funnel icon next to the title of the column (near top of your screen)
2) A filtering options box will pop up with options on how to filter the column

- Useful filtering columns:
  - Type
  - Timestamp
  - Description: Useful for checking only tagged items
  - Hash category: will get filled out if RVS – match hash values against hash databases
- Type Column
  - Will not get items with mismatched file signatures
  - Avoid with RVS option or by previewing a file

Sorting

- To sort a column (either ascending or descending), left click on the column title
- Can sort by up to 3 columns at once:
  - The primary sorted column will have a black triangle next to the column title, the secodndary column will have a dark grey triangle, and the tertiary column will have a light grey triangle
- Holding down shift and clicking on the column title will remove all other sorting

Report Table Associations

- To quickly add selected items to created report tables, press Ctrl and the corresponding number
- Used to group items

Creating a Report (better tagging) Instructions

1) Select the files you want to add to the report
2) Right click on one of the files and click "Report table association"
3) Click on New (unless you have previously created a group for the Items)
4) Select the group to add the tagged items too
5) Click Create
6) Click on file in the Case Data Window
7) Click on Create Report
8) In the top right select the Report Tables you want to include in your report
9) In the bottom right, select the specific details you want included in your report

Exporting Files - Instructions

1) Right click on the file you want to export
2) Click on Recover/Copy…
3) Input the desired output path

Exporting File Metadata

Must run RVS first for certain fields

1) Select the file(s) you want information from
2) Right click on any one of the selected files
3) Click export list
   - To copy selected fields to clipboard, select both TSV and clipboard
4) Select the fields you want to include
5) Click OK

Shifting Columns

1) Open the filtering settings (CRTL F5)
2) Click the circle on the far right of the column you want to shift
3) Using the up or down arrows in the top right of the window, move the column name up or down to the desired location