



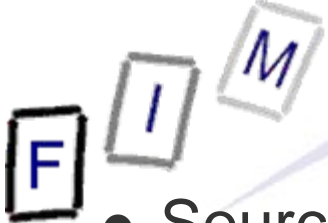
Mag. iur. Dr. techn. Michael Sonntag

Recovering web-browsing history

Security and Privacy
VSE Prag, 7 - 11.6.2010

Institute for Information Processing and
Microprocessor Technology (FIM)
Johannes Kepler University Linz, Austria

E-Mail: sonntag@fim.uni-linz.ac.at
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



- Source files: User profile of JDoe (extract only)
 - JDoe\Favorites
 - » Bookmarks
 - JDoe\Cookies
 - » Cookie directory
 - JDoe\Local Settings\History
 - » Visited URLs
 - JDoe\Local Settings\Temporary Internet Files
 - » Cache directory
 - HKCU_Software_Microsoft_Internet Explorer.reg
 - » Registry (HKCU or HKU\<User-SID>; IE part only)
- Requirements:
 - Software:
 - » Galleta
 - » Pasco
 - Registry editor

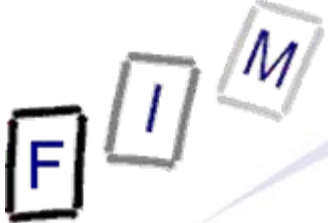


- Your tasks:
 - Investigate the bookmarks of the suspect
 - » Which sites did he visit?
 - » Did he add (which?) own bookmarks?
 - Produce a list of all bookmarks
- Source: The JDoe\Favorites folder

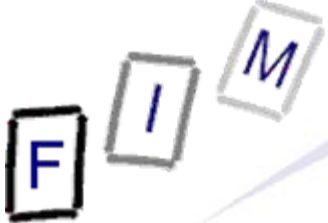
- Please note: The file date/time cannot be original any more because it had to be copied for this course!



- Your tasks:
 - Investigate the cookies of the suspect
 - » Which sites did he visit?
 - » Can we say which were visited intentionally?
 - Advertisement banners!
 - Produce a list of all sites with their visit time
- Sources:
 - The JDoe\Cookies folder
 - The index.dat file within
- Software:
 - Use "Pasco" for the index.dat file and import the results into a spreadsheet for better investigation
 - Use "Galleta" for individual cookie files
- Please note: The file date/time cannot be original any more because it had to be copied for this course!



- Your tasks:
 - Investigate the URLs the suspect visited
 - » Which sites did he visit?
 - » What can we find out about the actions on these sites?
 - Produce a list of all URLs with their visit time
- Sources:
 - The JDoe\Local Settings\History folder
 - The History.IE5\index.dat file within
- Software: Use "Pasco" for this and import the result to a spreadsheet for better investigation
- Please note: The file date/time cannot be original any more because it had to be copied for this course!



- Your tasks:
 - Investigate the cache for the E-Mail messages of the suspect
 - » Can we find out some content?
 - Investigate the shopping behaviour (Beate Uhse, Amazon)
- Sources:
 - The JDoe\Local Settings\Temporary Internet Files folder
 - The Content.IE5\index.dat file within
- Software: Use "Pasco" for this and import the result to a spreadsheet for better investigation
- Please note: The file dates/times cannot be original any more because it had to be copied for this course!



- Your tasks:
 - Check what URLs were entered manually
 - » These should match the sites visited, as we have found no bookmarks for them!
 - » These sites were obviously visited intentionally
 - No pop-ups, banners etc.!
- Sources:
 - HKCU_Software_Microsoft_Internet Explorer.reg
- Software: Use a text editor
 - Import to registry is not that ideal, as it is incomplete and would be added locally
 - » Would work better if it was a complete hive; could be "mounted"
- Please note: This is an export of a subtree. It only contains the data, but not associated information, like the last access date/time of keys!



Conclusions

- We can find out quite a lot about the suspect, especially through the cache
 - What he shopped for, his interests (wishlist)
 - His E-Mail address used at Amazon for registration
 - » Can be found again on GMX
- The registry provides information on explicit user actions
 - Allows removing the "automatic" displays → Ads
- Visited URLs: What the suspect searched for
 - Google search URLs
- Cookies did not provide a lot of useful information
 - Some IDs might help in combination with data from the websites, but these are not accessible for us here!

F I M

Questions?

Thank you for your attention!