Proj 13: Thumbcache (15 pts.)

Kebutuhan Project

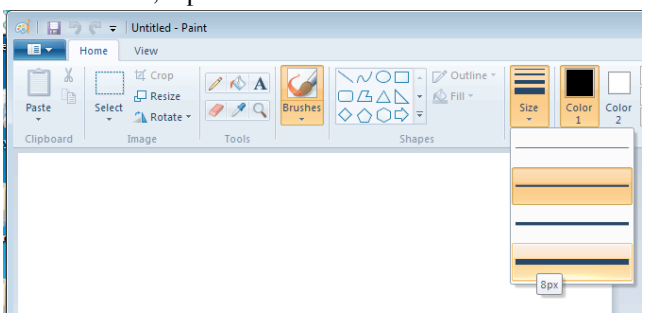
- Komputer Windows Vista, atau Windows 7, real atau virtual. Instruksi berikut menggunakan Windows 7 Virtual. Memungkinkan mengerjakan project ini menggunakan Windows XP, akan tetapi file thumbnail berbeda dan instruksi di sini tidak berjalan.

Tujuan

Saudara akan membuat dua gambar dan mendelete salah satunya. Kemudian me-recover evidence dari kedua gambar dari Thumbnail Cache.

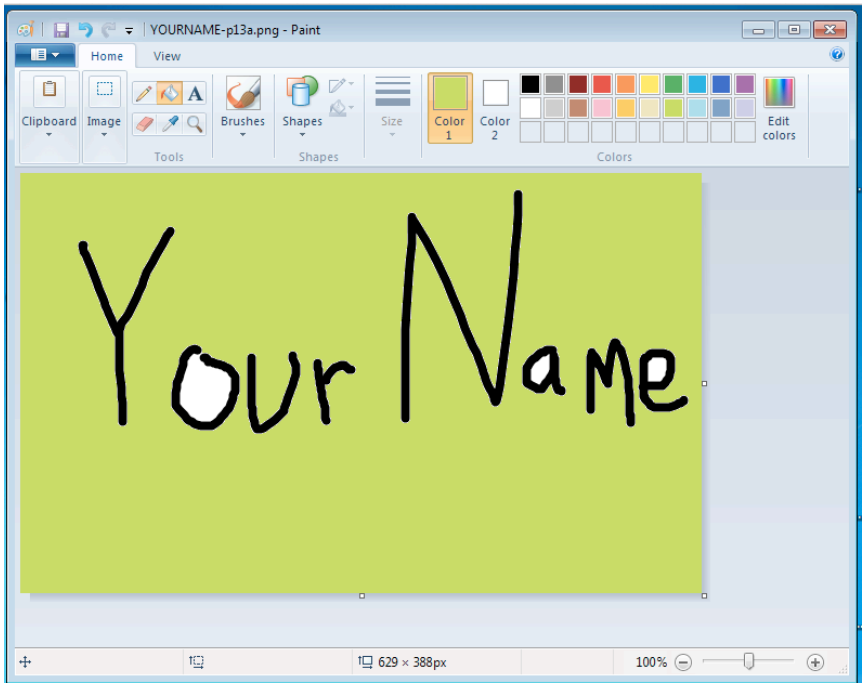
Membuat Dua Gambar Test

1. Buka Paint. Click icon pencil icon, dan rubah ketebalan baris dengan stingan yang paling tebal, seperti di bawah ini:

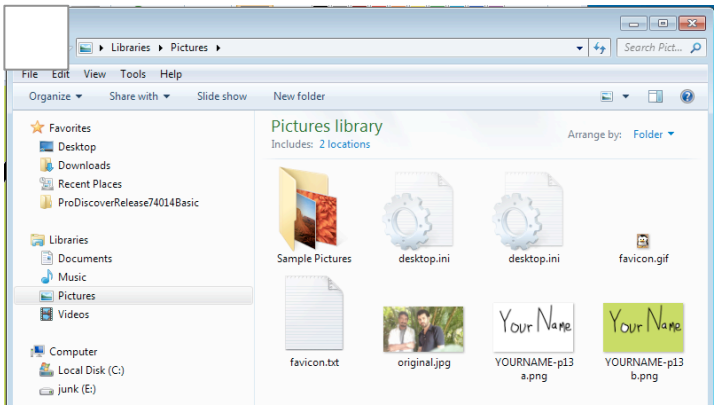


2. Tulis nama kalian menggunakan mouse, seperti terlihat di bawh ini. Gunakan nama masing-masing.

3. Simpan file pada folder Pictures dengan nama "NAMAKAMU-p13a". Gunakan nama masing-masing. Gunakan Tipe File PNG.
4. Click tool bucket, click warna apa saja, dan cat background dengan warna lain, seperti terlihat di bawah ini. Pastikan nama masih terbaca.



5. Simpan file pada folder Pictures, atau folder lain yang mudah dicari, dengan nama "NAMAKAMU-p13b". Gunakan jenis File Type PNG.
6. Tutup Paint.
7. Click **Start**, **Pictures**.
8. Akan terlihat dua thumbnail gambar dari kedua file yang baru dibuat, sperti berikut:



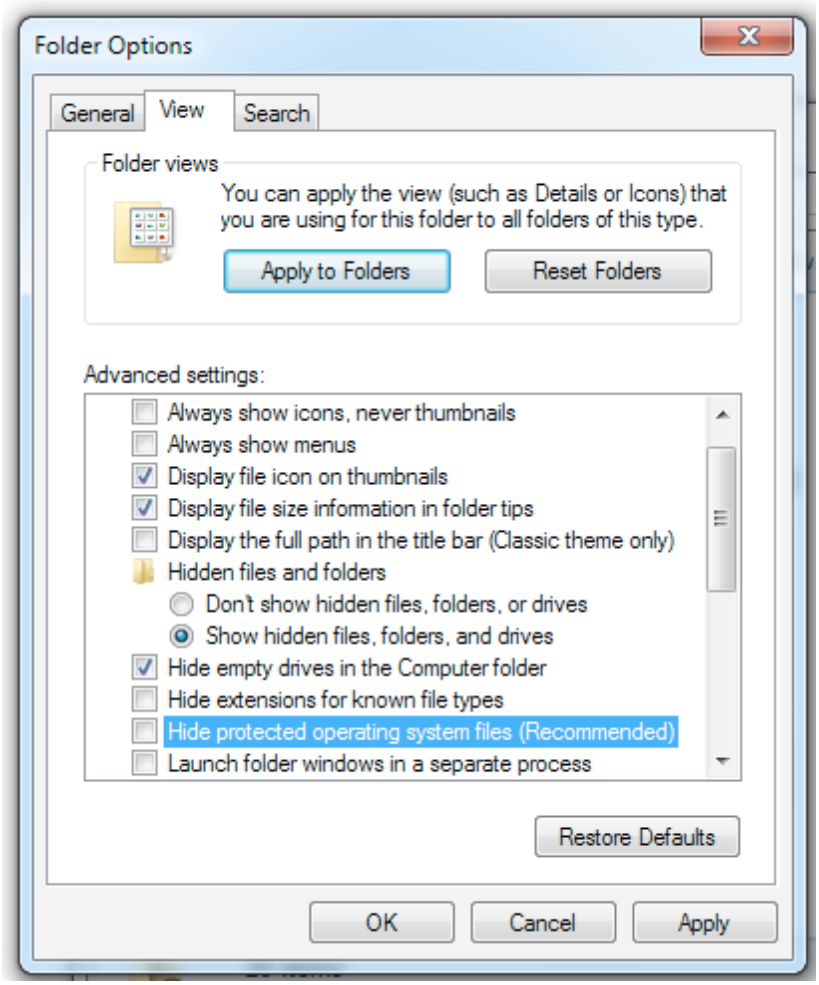
9. Drag file "NAMAKAMU-p15b" ke Recycle Bin
10. Klik kanan Recycle Bin dan click "**Empty recycle bin**". Click **Yes** untuk konfirmasi mendelete.

Melihat File Thumbcache

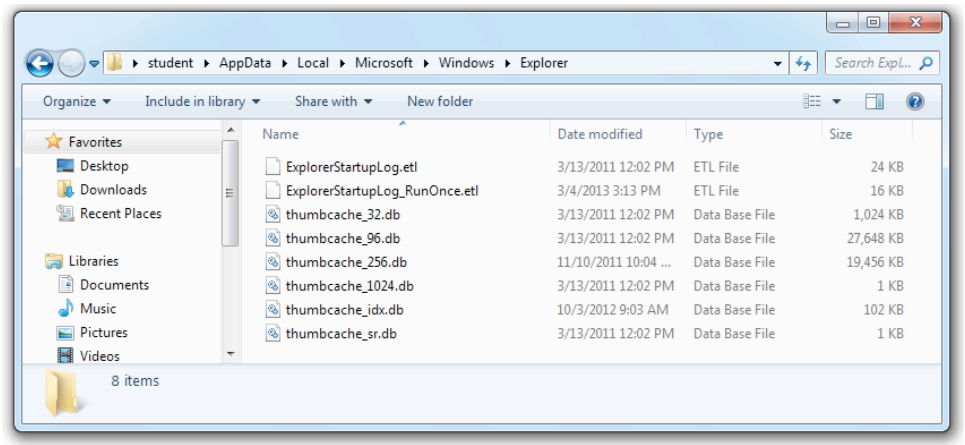
11. Click **Start**. Pada sisi kanan atas Start menu, click your logon name. Jika menggunakan lab Foresec, terlihat user **foresec**.
12. Pada jendela foresec, click **Organize**, "**Folder and search options**". Click tab **View**.
13. Buat dua pengaturan, seperti berikut:

- Click tombol "**Show hidden files, folders, or drives**"
- Bersihkan kotak "**Hide protected operating system files (Recommended)**".

14. Click **OK**.



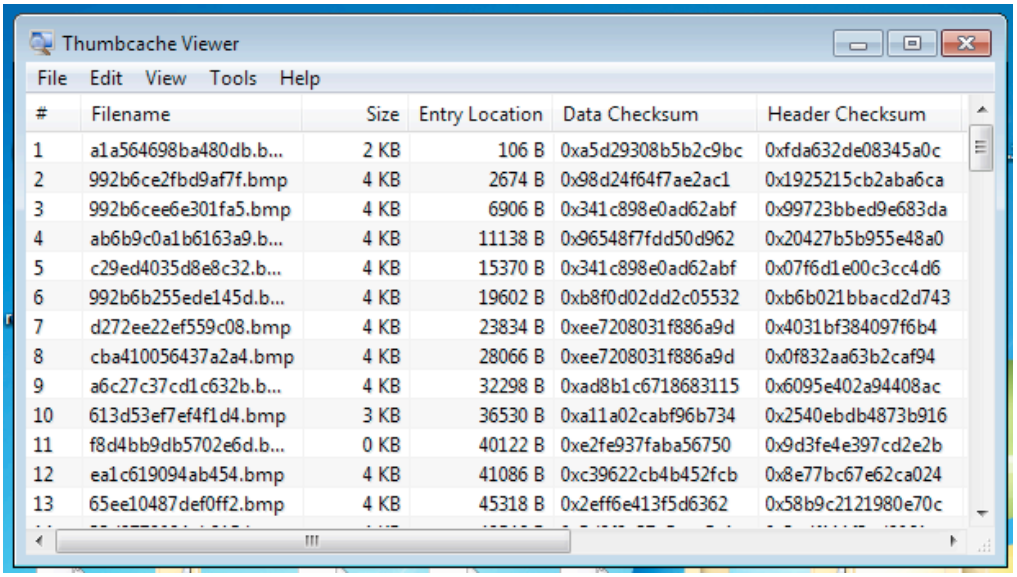
15. Pada jendela foresec, double-click **AppData**, **Local**, **Microsoft**, **Windows**, dan **Explorer**.
16. Akan terlihat beberapa file "thumbcache", seperti terlihat di bawah ini.



Download Thumbcache Viewer

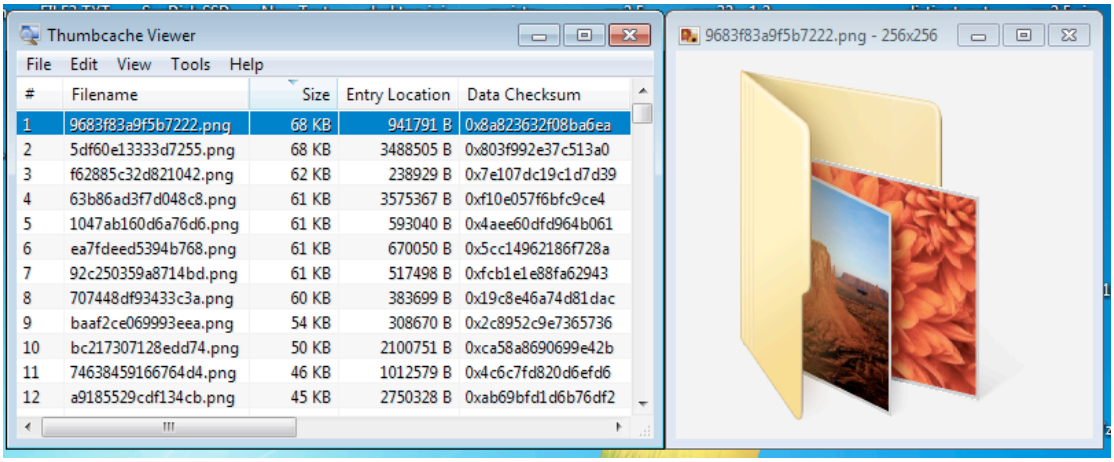
17. Untuk melihat file tersebut, buka Web browser dan arahkan ke https://code.google.com/p/thumbcache-viewer/ , atau bisa di download di elearning.
18. Click tab **Downloads**.
19. Download file **thumbcache_viewer.exe** dan jalankan.
20. Pada "Thumbcache Viewer", click **File**, **Open**.

21. Arahkan **C:\Users\foresec\AppData\Local\Microsoft\Windows\Explorer** dan double-click **thumbcache_256.db**. Jika mengerjakan di rumah Ganti nama "user" dengan username.
22. Sejumlah files dengan nama hexadecimal yang panjang muncul, seperti di bawah ini:



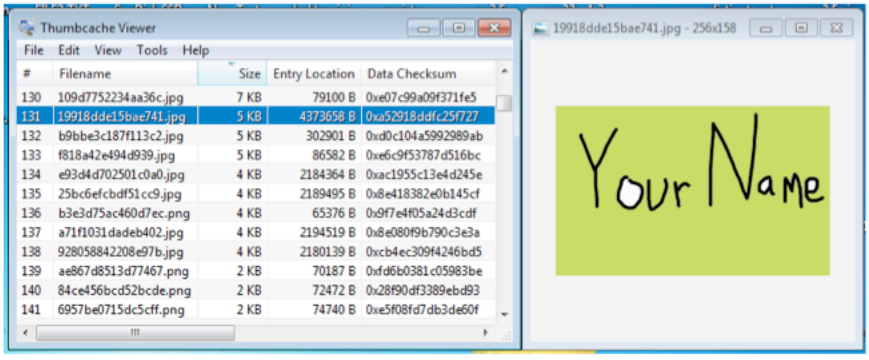
#	Filename	Size	Entry Location	Data Checksum	Header Checksum
1	a1a564698ba480db.b...	2 KB	106 B	0xa5d29308b5b2c9bc	0xfda632de08345a0c
2	992b6ce2fbd9af7f.bmp	4 KB	2674 B	0x98d24f64f7ae2ac1	0x1925215cb2aba6ca
3	992b6cee6e301fa5.bmp	4 KB	6906 B	0x341c898e0ad62abf	0x99723bbed9e683da
4	ab6b9c0a1b6163a9.b...	4 KB	11138 B	0x96548f7fdd50d962	0x20427b5b955e48a0
5	c29ed4035d8e8c32.b...	4 KB	15370 B	0x341c898e0ad62abf	0x07f6d1e00c3cc4d6
6	992b6b255ede145d.b...	4 KB	19602 B	0xb8f0d02dd2c05532	0xb6b021bbacd2d743
7	d272ee22ef559c08.bmp	4 KB	23834 B	0xee7208031f886a9d	0x4031bf384097f6b4
8	cba410056437a2a4.bmp	4 KB	28066 B	0xee7208031f886a9d	0x0f832aa63b2caf94
9	a6c27c37cd1c632b.b...	4 KB	32298 B	0xad8b1c6718683115	0x6095e402a94408ac
10	613d53ef7ef4f1d4.bmp	3 KB	36530 B	0xa11a02cabf96b734	0x2540ebdb4873b916
11	f8d4bb9db5702e6d.b...	0 KB	40122 B	0xe2fe937faba56750	0x9d3fe4e397cd2e2b
12	ea1c619094ab454.bmp	4 KB	41086 B	0xc39622cb4b452fcb	0x8e77bc67e62ca024
13	65ee10487def0ff2.bmp	4 KB	45318 B	0x2eff6e413f5d6362	0x58b9c2121980e70c

23. Beberapa gambar berukuran "Size" nol. Click **Size** column header abu abu untuk mengurutkan berdasarkan ukuran.
24. Click gambar yang paling besar.
25. Gambar muncul pada Image Viewer, seperti berikut:



#	Filename	Size	Entry Location	Data Checksum
1	9683f83a9f5b7222.png	68 KB	941791 B	0x8a823632f08ba6ea
2	5df60e13333d7255.png	68 KB	3488505 B	0x803f992e37c513a0
3	f62885c32d821042.png	62 KB	238929 B	0x7e107dc19c1d7d39
4	63b86ad3f7d048c8.png	61 KB	3575367 B	0xf10e057f6bfc9ce4
5	1047ab160d6a76d6.png	61 KB	593040 B	0x4aee60dfd964b061
6	ea7fdeed5394b768.png	61 KB	670050 B	0x5cc14962186f728a
7	92c250359a8714bd.png	61 KB	517498 B	0xfcb1e1e88fa62943
8	707448df93433c3a.png	60 KB	383699 B	0x19c8e46a74d81dac
9	baaf2ce069993eea.png	54 KB	308670 B	0x2c8952c9e7365736
10	bc217307128edd74.png	50 KB	2100751 B	0xca58a8690699e42b
11	74638459166764d4.png	46 KB	1012579 B	0x4c6c7fd820d6efd6
12	a9185529cdf134cb.png	45 KB	2750328 B	0xab69bfd1d6b76df2

26. Tekan tombol panah ke bawah untuk mencari gambar dengan nama kalian, seperti berikut ini:



#	Filename	Size	Entry Location	Data Checksum
130	109d7752234aa36c.jpg	7 KB	79100 B	0xe07c99a09f371fe5
131	19918dde15bae741.jpg	5 KB	4373658 B	0xa52918ddfc25f727
132	b9bbe3c187f113c2.jpg	5 KB	302901 B	0xd0c104a5992989ab
133	f818a42e494d939.jpg	5 KB	86582 B	0xe6c9f53787d516bc
134	e93d4d702501c0a0.jpg	4 KB	2184364 B	0xac1955c13e4d245e
135	25bc6efcbdf51cc9.jpg	4 KB	2189495 B	0x8e418382e0b145cf
136	b3e3d75ac460d7ec.png	4 KB	65376 B	0x9f7e4f05a24d3cdf
137	a71f1031dadeb402.jpg	4 KB	2194519 B	0x8e080f9b790c3e3a
138	928058842208e97b.jpg	4 KB	2180139 B	0xcb4ec309f4246bd5
139	ae867d8513d77467.png	2 KB	70187 B	0xfd6b0381c05983be
140	84ce456bcd52bcde.png	2 KB	72472 B	0x28f90df3389ebd93
141	6957be0715dc5cff.png	2 KB	74740 B	0xe5f08fd7db3de60f

27. Jika tidak ketemu gambar yang dicari, coba cari thumbcache files yang lain.

Simpan Screen Image

28. Pastikan di layar terlihat gambar dengan nama kalian.
29. Tekan PrintScrn pada bagian atas keyboard. Yang akan mengkopi seluruh desktop ke clipboard.

SUBMIT GAMBAR KESELURUHAN WHOLE DESKTOP UNTUK MENDAPAT POIN MAKSIMAL!

30. Simpan file dengan nama "**NAMAKAMU_Proj 13**". Gunakan nama masing-masing.

Mengumpulkan Project

31. Kirim di elearning.

Sumber

http://escforensics.blogspot.com/2012/11/analyzing-thumbcache.html
https://code.google.com/p/thumbcache-viewer/
http://www.woanware.co.uk/?page_id=89

Last Modified: 3-5-13