

Programma's zoals Winhex geven in dat geval als fileheader FILE0 aan.

Name	Size	Created	Modified	Accessed	Attr
Winhex.exe	3.8 KB	18-12-2007 18:14:57	18-12-2007 18:17:27	20-12-2007 13:13:32	A
Winhex.Prefetch	1.8 KB	17-11-2007 20:51:21	17-11-2007 09:51:21	20-12-2007 10:09:48	A
Winhex.Dat	3.8 KB	18-12-2007 20:38:10	18-12-2007 20:38:10	20-12-2007 13:02:05	A
Winhex.Dat	1.7 KB	18-12-2007 20:27:21	18-12-2007 20:27:21	20-12-2007 10:09:08	A

Hex	ASCII
454C3F88	FILE0
454C3F88	FILE0
454C3F88	FILE0

Zoals te zien is in dit voorbeeld (Winhex) staat de hele linkfile in de MFT. Het formaat van de linkfile is zo'n 600 bytes en de fileheader is FILE0. Alle bestanden in de MFT (dus niet alleen de linkfiles) hebben een fileheader FILE0. Als je een zoekopdracht zou doen naar FILE0 dan is het resultaat al snel enige tienduizenden cq. honderdduizenden treffers en zul je de linkfiles er niet snel tussenuit halen !

Desktop

C:\Documents and Settings\gebruikersnaam\Bureaublad

De Desktop map bevat snelkoppelingen naar de huidig geïnstalleerde en eerder geïnstalleerde (doch alweer gewijzigde) configuraties van het bureaublad. De snelkoppelingen refereren naar doelbestanden (applicaties, mappen, bestanden) of naar objecten zoals printers of externe harddisks. Elke snelkoppeling die in deze map staat wordt op het bureaublad vertegenwoordigd door een icoon. Als je op zo'n icoon op het bureaublad klikt dan wordt bijvoorbeeld een bestand gestart of een map geopend.

Als een bepaalde snelkoppeling aanwezig is op het bureaublad, dan maakt dat aannemelijk dat de eigenaar van de computer wist dat het bijbehorende programma of bestand op zijn computer aanwezig is / was. Tijdens de installatie van programma's wordt over het algemeen de optie geboden om een snelkoppeling op het bureaublad te plaatsen.

Belangrijke informatie

Zoals eerder genoemd registreert het besturingssysteem MAC tijden (Modified (last written), Accessed, Created) met betrekking tot de link files. Je kunt deze MAC tijden vergelijken met bijvoorbeeld de installatiedatum van het bijbehorende softwareprogramma of de map waarin het programma staat. Dan kan blijken dat de snelkoppeling is gemaakt nadat het programma op de computer is geïnstalleerd. De gebruiker heeft dan mogelijk opzettelijk de snelkoppeling op het bureaublad gemaakt en moet dan van het bestaan van het programma af hebben geweten. De snelkoppelingen in de Desktop map geven zicht op de configuratie van een computer op een bepaald tijdstip.

Menu Start

C:\Documents and Settings\gebruikersnaam\Menu Start

Tijdens de installatie van een softwareprogramma wordt over het algemeen een snelkoppeling gemaakt in het Start menu. De gebruiker kan er later zelf voor kiezen om deze snelkoppeling te verplaatsen naar het bureaublad (wat dan indiceert dat hij van het bestaan van het programma af moet hebben geweten).

De snelkoppelingen in de Start Menu map wijzen naar programma's en mappen die in het Windows start menu staan. Een snelkoppeling kan aanduiden dat een programma, dat nu niet meer op de computer aanwezig is, ooit geïnstalleerd is geweest. De datum en tijdstempels van de snelkoppeling kunnen helpen om te bepalen wanneer een applicatie geïnstalleerd is. Hun datum / tijd van creatie corresponderen met de datum van installatie. De snelkoppelingen bevatten ook het complete pad naar de bestanden die ze vertegenwoordigen.

Onlangs geopend

C:\Documents and Settings\gebruikersnaam\Onlangs geopend

De Onlangs geopend map bevat snelkoppelingen die wijzen naar bestanden die zijn geopend op de computer.

Standaard worden vijftien snelkoppelingen bijgehouden. Als een gebruiker klikt op op de Start knop en vervolgens Documents selecteert, dan toont het besturingssysteem een lijst van recent geopende bestanden. Als de gebruiker in deze lijst een keuze maakt, dan wordt het bestand geopend. De snelkoppelingen in deze map bevatten het complete pad naar het bestand. De snelkoppelingen kunnen aanduiden hoe de computer op een bepaalde datum en tijd was geconfigureerd. Een snelkoppeling kan refereren aan een volume dat niet beschikbaar was op het moment van onderzoek.

MAC tijden

De Created, Accessed en Modified (last written) tijden van het doelbestand zijn opgeslagen in byte offsets 28, 36 en 44 van de link file. Elke datum / tijd is 8 bytes lang en eindigt met 01h.

Je kunt met FTK Imager eenvoudig zien dat dit klopt. Ga bijvoorbeeld naar c:\Documents and Settings\gebruikersnaam\Bureaublad\bestand.lnk en ga (gemeten vanaf de eerste byte van dit bestand) naar de 28e byte. Selecteer vervolgens de 8 navolgende bytes en je eindigt op een 01h.

```

WinHex.lnk          1 KB Regular file
NAMPP Control Panel.lnk  1 KB Regular file

000 4c 00 00 00 01 14 02 00-00 00 00 00 c0 00 00 00 L.....Ã...
010 00 00 00 46 9b 00 00 00-20 00 00 00 ec 4e 11 84 ...F.....lH..
020 bc 3f c8 01 62 25 9a 51-02 40 c8 01 00 2c 46 bf 4eE-bd-Q-8E-.,Fç
030 08 38 c8 01 00 44 18 00-00 00 00 00 01 00 00 00 -8E-D.....
040 00 00 00 00 00 00 00 00-00 00 00 00 e9 00 14 00 .....é...
050 1f 50 e0 4f d0 20 ea 3a-69 10 a2 d8 08 00 2b 30 -P&O@:i-cD-+0
060 30 9d 19 00 2f 43 3a 5c-00 00 00 00 00 00 00 00 0-../C:\.....
070 00 00 00 00 00 00 00 00-00 00 00 00 34 00 31 00 00 .....4.1..
080 00 00 00 90 37 f1 83 10-00 74 65 6d 70 00 00 20 .....7d...temp-
090 00 03 00 04 00 ef be 4f-37 2b 85 90 37 f1 83 14 .....1N07---7d--
0a0 00 00 00 74 00 65 00 6d-00 70 00 00 00 14 00 40 .....t-e-m-p-----@

```

8 bytes vanaf byte offset 28

```

WinHex.lnk          1 KB Regular file
NAMPP Control Panel.lnk  1 KB Regular file

000 4c 00 00 00 01 14 02 00-00 00 00 00 c0 00 00 00 L.....Ã...
010 00 00 00 46 9b 00 00 00-20 00 00 00 ec 4e 11 84 ...F.....lH..
020 bc 3f c8 01 62 25 9a 51-02 40 c8 01 00 2c 46 bf 4eE-bd-Q-8E-.,Fç
030 08 38 c8 01 00 44 18 00-00 00 00 00 01 00 00 00 -8E-D.....
040 00 00 00 00 00 00 00 00-00 00 00 00 e9 00 14 00 .....é...
050 1f 50 e0 4f d0 20 ea 3a-69 10 a2 d8 08 00 2b 30 -P&O@:i-cD-+0
060 30 9d 19 00 2f 43 3a 5c-00 00 00 00 00 00 00 00 0-../C:\.....
070 00 00 00 00 00 00 00 00-00 00 00 00 34 00 31 00 00 .....4.1..
080 00 00 00 90 37 f1 83 10-00 74 65 6d 70 00 00 20 .....7d...temp-
090 00 03 00 04 00 ef be 4f-37 2b 85 90 37 f1 83 14 .....1N07---7d--
0a0 00 00 00 74 00 65 00 6d-00 70 00 00 00 14 00 40 .....t-e-m-p-----@

```

8 bytes vanaf byte offset 36

```

WinHex.lnk          1 KB Regular file
NAMPP Control Panel.lnk  1 KB Regular file

000 4c 00 00 00 01 14 02 00-00 00 00 00 c0 00 00 00 L.....Ã...
010 00 00 00 46 9b 00 00 00-20 00 00 00 ec 4e 11 84 ...F.....lH..
020 bc 3f c8 01 62 25 9a 51-02 40 c8 01 00 2c 46 bf 4eE-bd-Q-8E-.,Fç
030 08 38 c8 01 00 44 18 00-00 00 00 00 01 00 00 00 -8E-D.....
040 00 00 00 00 00 00 00 00-00 00 00 00 e9 00 14 00 .....é...
050 1f 50 e0 4f d0 20 ea 3a-69 10 a2 d8 08 00 2b 30 -P&O@:i-cD-+0
060 30 9d 19 00 2f 43 3a 5c-00 00 00 00 00 00 00 00 0-../C:\.....
070 00 00 00 00 00 00 00 00-00 00 00 00 34 00 31 00 00 .....4.1..
080 00 00 00 90 37 f1 83 10-00 74 65 6d 70 00 00 20 .....7d...temp-
090 00 03 00 04 00 ef be 4f-37 2b 85 90 37 f1 83 14 .....1N07---7d--
0a0 00 00 00 74 00 65 00 6d-00 70 00 00 00 14 00 40 .....t-e-m-p-----@

```

8 bytes vanaf byte offset 44

Met andere woorden, beginnende met byte offset 28 kun je 24 bytes selecteren. Deze 24 bytes bevatten de MAC tijden van de linkfile.

Binnen Encase kun je de MAC tijden eenvoudig opvragen. Met dit programma kun je ook de genoemde 24 bytes selecteren (dus beginnende met byte offset 28). Klik met de rechtermuisknop, selecteer Bookmark data en kies voor Windows date / time.

Let op: als je een volume bekijkt dat met Fat is gemaakt, dan wordt de tijd niet juist getoond. Dat komt omdat

FAT, in tegenstelling tot NTFS, alleen de datum opslaat.

Serienummer

Om te bepalen of een bestand origineel is opgeslagen op het volume dat je aan het onderzoeken bent, dan kun je gebruik maken van de Volume Serial Number. Dit is een sinds 1987 standaard aanwezige, doch voor elk volume unieke waarde, die werd gegeven toen het volume werd geformatteerd, op basis van datum/tijd van formatteren en andere factoren.

Helaas kun je het Volume Serial Number niet zomaar terugvinden en decoderen. Tools zoals FTK Imager en Encase kunnen het serienummer voor je opzoeken.

File System Information	
Cluster Size	4,096
Cluster Count	14,649,382
Free Cluster Count	2,238,775
Dirty Flag	<input type="checkbox"/>
Volume Serial Number	CCES-909A
File System version	Windows XP (NTFS 3.1)
UTC Timestamps	<input checked="" type="checkbox"/>

Volume Serial Number, gevonden door FTK Imager

Om het serienummer met Encase te vinden moet je kijken naar 10h voor het volume label. De vier bytes voor deze 10h bevatten het volume serienummer, in little endian formaat. Kies voor rechtermuisknop – Bookmark – kies voor optie Integers: 32 bit integer – en je ziet het serienummer staan onder Hex. Je kunt nu dit serienummer vergelijken met het serienummer van het volume dat je aan het onderzoeken bent. Klik hiertoe (in de Cases – Entries – Home view) op Devices (in de tree pane). Klik vervolgens op het volume dat je wilt onderzoeken (in de table pane) en klik op Report view (in de view pane). Het serienummer komt nu tevoorschijn in het rapport en moet overeenkomen met het serienummer dat je zojuist bij de snelkoppeling hebt aangetroffen. Als de serienummers overeenkomen, dan betekent dat dat de snelkoppeling is gemaakt op het volume dat je aan het onderzoeken bent.

Als je zelf het Volume Serial Number wilt berekenen (het kan namelijk wel), dan kun je [hier een goede handleiding vinden](#).

De meest duidelijke aanwezigheid van linkfiles vind je in de unallocated clusters. Een groot voordeel van NTFS is dat de inhoud van kleine bestanden (zoals kleine .lnk bestanden) compleet in de MFT wordt opgeslagen. Verwijderde snelkoppelingbestanden zijn hierdoor nog direct leesbaar. Clusters in het unallocated gebied van het volume kunnen ook snelkoppelingbestanden bevatten, ook al is er geen map of MFT meer die de link kan identificeren (zie bovenaan onder fileheaders).

Parzen met Encase

Om met Encase alle informatie in linkbestanden te decoderen kun je gebruik maken van de Case Processor EnScript module en kiezen voor Link File Parser.

Doscommando

Het Volume Serial Number van een disk vind je eenvoudig via het doscommando vol dat je in een dosbox kunt uitvoeren.

Pad naar bestand

De inhoud van een linkfile is redelijk eenvoudig te lezen, bijvoorbeeld met FTK Imager. Je ziet dan bijvoorbeeld het originele pad naar het bestand.

```

0e0 00 68 00 65 00 78 00 31-00 34 00 00 00 18 00 4e -h-e-x-1-4-....F
0f0 00 32 00 00 44 18 00 86-37 c0 e8 20 00 57 49 6e -2-D-..7ah-^Min
100 48 65 78 2e 68 78 45 00-00 2c 00 03 00 04 00 ef Hex.exe+.,....I
110 be 90 37 8f 42 90 37 05-88 14 00 00 00 57 00 69 %7-B-7-....N-I
120 00 6e 00 48 00 65 00 78-00 2e 00 65 00 78 00 65 +h-e-x-..e-x-e
130 00 00 00 1a 00 00 00 4a-00 00 00 1c 00 00 00 01 .....J.....
140 00 00 00 1c 00 00 00 2d-00 00 00 00 00 00 00 49 .....I.....
150 00 00 00 11 00 00 00 03-00 00 00 9a 90 e5 ee 10 .....4I-
160 00 00 00 00 43 3a 5c 74-65 6d 70 5c 77 69 6e 68 ----C:\temp\Winh
170 65 78 31 34 5c 57 69 6e-48 65 78 2e 65 78 65 00 ex14\WinHex.exe+
180 00 21 00 2e 00 2e 00 5c-00 2e 00 2e 00 5c 00 2e !-..-..-..-..-
190 00 2e 00 5c 00 74 00 65-00 6d 00 70 00 5c 00 77 .-.\-temp\w
1a0 00 69 00 6e 00 68 00 65-00 78 00 31 00 34 00 5c -i-n-h-e-x-1-4-
1b0 00 57 00 69 00 6e 00 48-00 65 00 78 00 2e 00 65 -N-i-n-h-e-x-..e
1c0 00 78 00 65 00 10 00 43-00 3a 00 5c 00 74 00 65 x-e-+C-+h-+s-e

```

Pad in een linkfile, bekeken met FTK Imager.

Mocht je, in het geval dat een belangrijk bestand al gewist of gewiped is, het geluk hebben dat de linkfile nog aanwezig is in de MFT of in de unallocated clusters, dan kun je op deze manier eenvoudig zien waar het oorspronkelijke bestand heeft gestaan.

Name	Dir	Size	Created	Modified	Accessed	Attr	Index
WinHex.lnk	lnk	0.5 KB	16-12-2007 19:16:57	16-12-2007 18:17:22	20-12-2007 10:13:02	A	3086564
Mostly Photos.lnk	lnk	1.8 KB	17-12-2007 09:11:21	17-12-2007 09:11:21	20-12-2007 10:09:48	A	1804938
Magoo Desktop.lnk	lnk	0.5 KB	12-12-2007 20:38:15	12-12-2007 20:38:15	20-12-2007 10:02:05	A	1804938
Live View Desktop.lnk	lnk	1.7 KB	16-12-2007 00:07:20	16-12-2007 00:07:21	20-12-2007 10:02:05	A	1804938

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
484C2F28	00	00	00	11	00	00	00	00	00	00	00	00	00	00	00	00
484C2F29	65	78	31	34	5C	57	69	6E	48	65	78	2E	65	78	65	00
484C2F2A	00	21	00	2E	00	2E	00	5C	00	2E	00	2E	00	5C	00	2E

Pad in een linkfile, bekeken met Winhex.

Winhex geeft meer informatie, zoals de MAC tijden van de linkfile en het pad naar het originele bestand dat wordt cq. werd vertegenwoordigd. Als je hierbij vanaf byte offset 28 nog de MAC tijden van het vertegenwoordigde bestand weet te vinden (een reeks van 24 bytes, zoals hierboven omschreven) dan is je informatie vrijwel compleet.

Meer informatie

<http://www.forensicfocus.com/link-file-evidentiary-value>

http://www.i2s-lab.com/Papers/The_Windows_Shortcut_File_Format.pdf