

COMP 5350 / 6350

Digital Forensics

Timeline Analysis

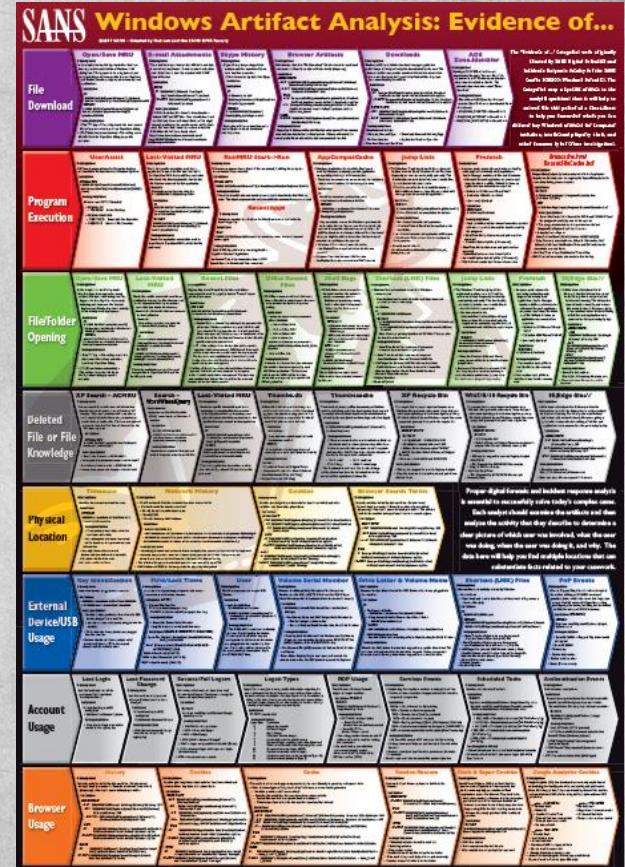


Event Timelines

- By consolidating different digital artifacts collected during a forensics analysis we can generate a list of events based on user, date/time, and source
 - ✓ File Modification
 - Created
 - Accessed
 - Copied
 - ✓ Operating System Modification
 - Registry
 - File System
 - ✓ Event Logs
 - ✓ Application Execution
 - ✓ Device Connections

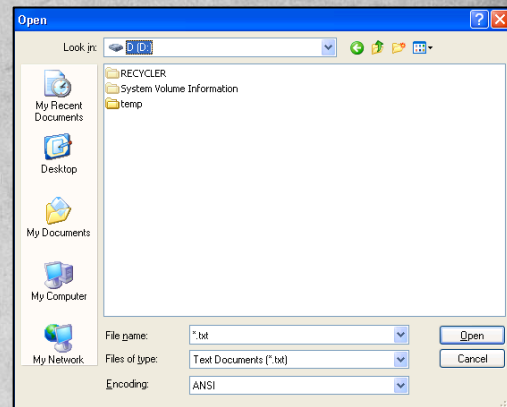
SANS Artifact Analysis

- The SANS institute provides a wide variety of technical training across numerous cybersecurity domains
- SANS has mapped digital artifacts in the Windows OS along with their storage location in the file system
 - ✓ File Download
 - ✓ Program Execution
 - ✓ File Opening / Creation
 - ✓ Deleted File / File Knowledge
 - ✓ Physical Location
 - ✓ USB / Drive Usage
 - ✓ Account Usage
 - ✓ Browser Usage



File Download – Open / Save MRU

- Tracks files opened or saved within a Windows shell dialog box
- Includes web browser and application keys
 - ✓ “*” key: Subkey that tracks most recent files of any extension input in an OpenSave dialog
 - ✓ *.???: Subkey stores file info from OpenSave dialog by specific extension



NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDIMRU

File Download	Open/Save MRU	E-mail Attachments	Skype History	Browser Artifacts	Downloads	ADS Zone.Identifier
	<p>Description:</p> <p>In the simplest terms, this key tracks files that have been opened or saved within a Windows shell dialog box. This happens to be a big data set, not only including web browsers like Internet Explorer and Firefox, but also a majority of commonly used applications.</p> <p>Location:</p> <p>XP NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU</p> <p>Win7/8 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDIMRU</p> <p>Interpretation:</p> <ul style="list-style-type: none">• The “*” key: This subkey tracks the most recent files of any extension input in an OpenSave dialog.• *.??? (Three letter extension): This subkey stores file info from the OpenSave dialog by specific extension.	<p>Description:</p> <p>The e-mail industry estimates that 80% of e-mail data is stored via attachments. E-mail standards only allow text. Attachments must be encoded with MIME/ base64 format.</p> <p>Location:</p> <p>Outlook XP %USERPROFILE%\Local Settings\ApplicationData\Microsoft\Outlook</p> <p>Win7/8 %USERPROFILE%\AppData\Local\Microsoft\Outlook</p> <p>Interpretation:</p> <p>MS Outlook data files found in these locations include OST and PST files. One should also check the OUK and ContentOutlook folder, which might roam depending on the specific version of Outlook used. For more information on where to find the OUK folder, this link has a handy chart: http://www.hancockcomputerstech.com/blog/2010/01/06/find-the-microsoft-outlook-temporary-ouk-folder</p>	<p>Description:</p> <ul style="list-style-type: none">• Skype history keeps a log of chat sessions and files transferred from one machine to another.• This is turned on by default in Skype installations. <p>Location:</p> <p>XP C:\Documents and Settings\%username%\Application\Skype\%skype-name%</p> <p>Win7/8 C:\%USERPROFILE%\AppData\Roaming\Skype\%skype-name%</p> <p>Interpretation:</p> <p>Each entry will have a date/time value and a Skype username associated with the action.</p>	<p>Description:</p> <p>Not directly related to “File Download”. Details stored for each local user account. Records number of times visited (frequency).</p> <p>Location:</p> <p>Internet Explorer: - IE9-9 %USERPROFILE%\AppData\Roaming\Microsoft\Windows\History\History\index.dat - IE10-11 %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCache*.dat</p> <p>Firefox: - v25 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\%random text%.default\downloads.sqlite - v26+ %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\%random text%.default\places.sqlite Table:moz_annos</p> <p>Chrome: - Win7/8 %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History</p> <p>Interpretation:</p> <p>Many sites in history will list the files that were opened from remote sites and downloaded to the local system. History will record the access to the file on the website that was accessed via a link.</p>	<p>Description:</p> <p>Firefox and IE has a built-in download manager application which keeps a history of every file downloaded by the user. This browser artifact can provide excellent information about what sites a user has been visiting and what kinds of files they have been downloading from them.</p> <p>Location:</p> <p>Firefox: - XP %userprofile%\Application Data\Mozilla\Firefox\Profiles\%random text%.default\downloads.sqlite - Win7/8 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\%random text%.default\downloads.sqlite</p> <p>Internet Explorer: - IE8-9 %USERPROFILE%\AppData\Roaming\Microsoft\Windows\History\History\index.dat - IE10-11 %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCache*.dat</p> <p>Interpretation:</p> <p>Downloads will include:</p> <ul style="list-style-type: none">• Filename, Size, and Type• File Save Location• Download from and Referring Page• Application Used to Open File• Download Start and End Times	<p>Description:</p> <p>Starting with XP SP2 when files are downloaded from the “Internet Zone” via a browser to a NTFS volume, an alternate data stream is added to the file. The alternate data stream is named “Zone.Identifier”.</p> <p>Interpretation:</p> <p>Files with an ADS Zone.Identifier and contains ZoneID=3 were downloaded from the Internet</p> <ul style="list-style-type: none">• URLZONE_TRUSTED = ZoneID = 2• URLZONE_INTERNET = ZoneID = 3• URLZONE_UNTRUSTED = ZoneID = 4

File Download – Browser Artifacts

- Not directly related to “File Download” MRU, but is maintained in each user account
- Shows files opened from remote sites and downloaded to local system
- Records file access on the website that was accessed through a link
- Browser History Locations:

✓ IE 10 & 11:

%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

✓ Chrome:

%USERPROFILE%\AppData\Local\Google\Chrome\UserData\Default\History

File Download

Open/Save MRU

Description

In the simplest terms, this key tracks files that have been opened or saved using a Windows Explorer dialog box. This happens to be a log data set not usually found by browsers or other forensic tools, and Firefox, but also a majority of commonly used applications.

Location:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\{Open|Save|Print}
```

Index

```
MRUOpen
MRUOpen2
MRUOpen3
MRUOpen4
MRUOpen5
MRUOpen6
MRUOpen7
MRUOpen8
MRUOpen9
MRUOpen10
MRUOpen11
MRUOpen12
MRUOpen13
MRUOpen14
MRUOpen15
MRUOpen16
MRUOpen17
MRUOpen18
MRUOpen19
MRUOpen20
MRUOpen21
MRUOpen22
MRUOpen23
MRUOpen24
MRUOpen25
MRUOpen26
MRUOpen27
MRUOpen28
MRUOpen29
MRUOpen30
MRUOpen31
MRUOpen32
MRUOpen33
MRUOpen34
MRUOpen35
MRUOpen36
MRUOpen37
MRUOpen38
MRUOpen39
MRUOpen40
MRUOpen41
MRUOpen42
MRUOpen43
MRUOpen44
MRUOpen45
MRUOpen46
MRUOpen47
MRUOpen48
MRUOpen49
MRUOpen50
MRUOpen51
MRUOpen52
MRUOpen53
MRUOpen54
MRUOpen55
MRUOpen56
MRUOpen57
MRUOpen58
MRUOpen59
MRUOpen60
MRUOpen61
MRUOpen62
MRUOpen63
MRUOpen64
MRUOpen65
MRUOpen66
MRUOpen67
MRUOpen68
MRUOpen69
MRUOpen70
MRUOpen71
MRUOpen72
MRUOpen73
MRUOpen74
MRUOpen75
MRUOpen76
MRUOpen77
MRUOpen78
MRUOpen79
MRUOpen80
MRUOpen81
MRUOpen82
MRUOpen83
MRUOpen84
MRUOpen85
MRUOpen86
MRUOpen87
MRUOpen88
MRUOpen89
MRUOpen90
MRUOpen91
MRUOpen92
MRUOpen93
MRUOpen94
MRUOpen95
MRUOpen96
MRUOpen97
MRUOpen98
MRUOpen99
MRUOpen100
MRUOpen101
MRUOpen102
MRUOpen103
MRUOpen104
MRUOpen105
MRUOpen106
MRUOpen107
MRUOpen108
MRUOpen109
MRUOpen110
MRUOpen111
MRUOpen112
MRUOpen113
MRUOpen114
MRUOpen115
MRUOpen116
MRUOpen117
MRUOpen118
MRUOpen119
MRUOpen120
MRUOpen121
MRUOpen122
MRUOpen123
MRUOpen124
MRUOpen125
MRUOpen126
MRUOpen127
MRUOpen128
MRUOpen129
MRUOpen130
MRUOpen131
MRUOpen132
MRUOpen133
MRUOpen134
MRUOpen135
MRUOpen136
MRUOpen137
MRUOpen138
MRUOpen139
MRUOpen140
MRUOpen141
MRUOpen142
MRUOpen143
MRUOpen144
MRUOpen145
MRUOpen146
MRUOpen147
MRUOpen148
MRUOpen149
MRUOpen150
MRUOpen151
MRUOpen152
MRUOpen153
MRUOpen154
MRUOpen155
MRUOpen156
MRUOpen157
MRUOpen158
MRUOpen159
MRUOpen160
MRUOpen161
MRUOpen162
MRUOpen163
MRUOpen164
MRUOpen165
MRUOpen166
MRUOpen167
MRUOpen168
MRUOpen169
MRUOpen170
MRUOpen171
MRUOpen172
MRUOpen173
MRUOpen174
MRUOpen175
MRUOpen176
MRUOpen177
MRUOpen178
MRUOpen179
MRUOpen180
MRUOpen181
MRUOpen182
MRUOpen183
MRUOpen184
MRUOpen185
MRUOpen186
MRUOpen187
MRUOpen188
MRUOpen189
MRUOpen190
MRUOpen191
MRUOpen192
MRUOpen193
MRUOpen194
MRUOpen195
MRUOpen196
MRUOpen197
MRUOpen198
MRUOpen199
MRUOpen200
MRUOpen201
MRUOpen202
MRUOpen203
MRUOpen204
MRUOpen205
MRUOpen206
MRUOpen207
MRUOpen208
MRUOpen209
MRUOpen210
MRUOpen211
MRUOpen212
MRUOpen213
MRUOpen214
MRUOpen215
MRUOpen216
MRUOpen217
MRUOpen218
MRUOpen219
MRUOpen220
MRUOpen221
MRUOpen222
MRUOpen223
MRUOpen224
MRUOpen225
MRUOpen226
MRUOpen227
MRUOpen228
MRUOpen229
MRUOpen230
MRUOpen231
MRUOpen232
MRUOpen233
MRUOpen234
MRUOpen235
MRUOpen236
MRUOpen237
MRUOpen238
MRUOpen239
MRUOpen240
MRUOpen241
MRUOpen242
MRUOpen243
MRUOpen244
MRUOpen245
MRUOpen246
MRUOpen247
MRUOpen248
MRUOpen249
MRUOpen250
MRUOpen251
MRUOpen252
MRUOpen253
MRUOpen254
MRUOpen255
MRUOpen256
MRUOpen257
MRUOpen258
MRUOpen259
MRUOpen260
MRUOpen261
MRUOpen262
MRUOpen263
MRUOpen264
MRUOpen265
MRUOpen266
MRUOpen267
MRUOpen268
MRUOpen269
MRUOpen270
MRUOpen271
MRUOpen272
MRUOpen273
MRUOpen274
MRUOpen275
MRUOpen276
MRUOpen277
MRUOpen278
MRUOpen279
MRUOpen280
MRUOpen281
MRUOpen282
MRUOpen283
MRUOpen284
MRUOpen285
MRUOpen286
MRUOpen287
MRUOpen288
MRUOpen289
MRUOpen290
MRUOpen291
MRUOpen292
MRUOpen293
MRUOpen294
MRUOpen295
MRUOpen296
MRUOpen297
MRUOpen298
MRUOpen299
MRUOpen300
MRUOpen301
MRUOpen302
MRUOpen303
MRUOpen304
MRUOpen305
MRUOpen306
MRUOpen307
MRUOpen308
MRUOpen309
MRUOpen310
MRUOpen311
MRUOpen312
MRUOpen313
MRUOpen314
MRUOpen315
MRUOpen316
MRUOpen317
MRUOpen318
MRUOpen319
MRUOpen320
MRUOpen321
MRUOpen322
MRUOpen323
MRUOpen324
MRUOpen325
MRUOpen326
MRUOpen327
MRUOpen328
MRUOpen329
MRUOpen330
MRUOpen331
MRUOpen332
MRUOpen333
MRUOpen334
MRUOpen335
MRUOpen336
MRUOpen337
MRUOpen338
MRUOpen339
MRUOpen340
MRUOpen341
MRUOpen342
MRUOpen343
MRUOpen344
MRUOpen345
MRUOpen346
MRUOpen347
MRUOpen348
MRUOpen349
MRUOpen350
MRUOpen351
MRUOpen352
MRUOpen353
MRUOpen354
MRUOpen355
MRUOpen356
MRUOpen357
MRUOpen358
MRUOpen359
MRUOpen360
MRUOpen361
MRUOpen362
MRUOpen363
MRUOpen364
MRUOpen365
MRUOpen366
MRUOpen367
MRUOpen368
MRUOpen369
MRUOpen370
MRUOpen371
MRUOpen372
MRUOpen373
MRUOpen374
MRUOpen375
MRUOpen376
MRUOpen377
MRUOpen378
MRUOpen379
MRUOpen380
MRUOpen381
MRUOpen382
MRUOpen383
MRUOpen384
MRUOpen385
MRUOpen386
MRUOpen387
MRUOpen388
MRUOpen389
MRUOpen390
MRUOpen391
MRUOpen392
MRUOpen393
MRUOpen394
MRUOpen395
MRUOpen396
MRUOpen397
MRUOpen398
MRUOpen399
MRUOpen400
MRUOpen401
MRUOpen402
MRUOpen403
MRUOpen404
MRUOpen405
MRUOpen406
MRUOpen407
MRUOpen408
MRUOpen409
MRUOpen410
MRUOpen411
MRUOpen412
MRUOpen413
MRUOpen414
MRUOpen415
MRUOpen416
MRUOpen417
MRUOpen418
MRUOpen419
MRUOpen420
MRUOpen421
MRUOpen422
MRUOpen423
MRUOpen424
MRUOpen425
MRUOpen426
MRUOpen427
MRUOpen428
MRUOpen429
MRUOpen430
MRUOpen431
MRUOpen432
MRUOpen433
MRUOpen434
MRUOpen435
MRUOpen436
MRUOpen437
MRUOpen438
MRUOpen439
MRUOpen440
MRUOpen441
MRUOpen442
MRUOpen443
MRUOpen444
MRUOpen445
MRUOpen446
MRUOpen447
MRUOpen448
MRUOpen449
MRUOpen450
MRUOpen451
MRUOpen452
MRUOpen453
MRUOpen454
MRUOpen455
MRUOpen456
MRUOpen457
MRUOpen458
MRUOpen459
MRUOpen460
MRUOpen461
MRUOpen462
MRUOpen463
MRUOpen464
MRUOpen465
MRUOpen466
MRUOpen467
MRUOpen468
MRUOpen469
MRUOpen470
MRUOpen471
MRUOpen472
MRUOpen473
MRUOpen474
MRUOpen475
MRUOpen476
MRUOpen477
MRUOpen478
MRUOpen479
MRUOpen480
MRUOpen481
MRUOpen482
MRUOpen483
MRUOpen484
MRUOpen485
MRUOpen486
MRUOpen487
MRUOpen488
MRUOpen489
MRUOpen490
MRUOpen491
MRUOpen492
MRUOpen493
MRUOpen494
MRUOpen495
MRUOpen496
MRUOpen497
MRUOpen498
MRUOpen499
MRUOpen500
MRUOpen501
MRUOpen502
MRUOpen503
MRUOpen504
MRUOpen505
MRUOpen506
MRUOpen507
MRUOpen508
MRUOpen509
MRUOpen510
MRUOpen511
MRUOpen512
MRUOpen513
MRUOpen514
MRUOpen515
MRUOpen516
MRUOpen517
MRUOpen518
MRUOpen519
MRUOpen520
MRUOpen521
MRUOpen522
MRUOpen523
MRUOpen524
MRUOpen525
MRUOpen526
MRUOpen527
MRUOpen528
MRUOpen529
MRUOpen530
MRUOpen531
MRUOpen532
MRUOpen533
MRUOpen534
MRUOpen535
MRUOpen536
MRUOpen537
MRUOpen538
MRUOpen539
MRUOpen540
MRUOpen541
MRUOpen542
MRUOpen543
MRUOpen544
MRUOpen545
MRUOpen546
MRUOpen547
MRUOpen548
MRUOpen549
MRUOpen550
MRUOpen551
MRUOpen552
MRUOpen553
MRUOpen554
MRUOpen555
MRUOpen556
MRUOpen557
MRUOpen558
MRUOpen559
MRUOpen560
MRUOpen561
MRUOpen562
MRUOpen563
MRUOpen564
MRUOpen565
MRUOpen566
MRUOpen567
MRUOpen568
MRUOpen569
MRUOpen570
MRUOpen571
MRUOpen572
MRUOpen573
MRUOpen574
MRUOpen575
MRUOpen576
MRUOpen577
MRUOpen578
MRUOpen579
MRUOpen580
MRUOpen581
MRUOpen582
MRUOpen583
MRUOpen584
MRUOpen585
MRUOpen586
MRUOpen587
MRUOpen588
MRUOpen589
MRUOpen590
MRUOpen591
MRUOpen592
MRUOpen593
MRUOpen594
MRUOpen595
MRUOpen596
MRUOpen597
MRUOpen598
MRUOpen599
MRUOpen600
MRUOpen601
MRUOpen602
MRUOpen603
MRUOpen604
MRUOpen605
MRUOpen606
MRUOpen607
MRUOpen608
MRUOpen609
MRUOpen610
MRUOpen611
MRUOpen612
MRUOpen613
MRUOpen614
MRUOpen615
MRUOpen616
MRUOpen617
MRUOpen618
MRUOpen619
MRUOpen620
MRUOpen621
MRUOpen622
MRUOpen623
MRUOpen624
MRUOpen625
MRUOpen626
MRUOpen627
MRUOpen628
MRUOpen629
MRUOpen630
MRUOpen631
MRUOpen632
MRUOpen633
MRUOpen634
MRUOpen635
MRUOpen636
MRUOpen637
MRUOpen638
MRUOpen639
MRUOpen640
MRUOpen641
MRUOpen642
MRUOpen643
MRUOpen644
MRUOpen645
MRUOpen646
MRUOpen647
MRUOpen648
MRUOpen649
MRUOpen650
MRUOpen651
MRUOpen652
MRUOpen653
MRUOpen654
MRUOpen655
MRUOpen656
MRUOpen657
MRUOpen658
MRUOpen659
MRUOpen660
MRUOpen661
MRUOpen662
MRUOpen663
MRUOpen664
MRUOpen665
MRUOpen666
MRUOpen667
MRUOpen668
MRUOpen669
MRUOpen670
MRUOpen671
MRUOpen672
MRUOpen673
MRUOpen674
MRUOpen675
MRUOpen676
MRUOpen677
MRUOpen678
MRUOpen679
MRUOpen680
MRUOpen681
MRUOpen682
MRUOpen683
MRUOpen684
MRUOpen685
MRUOpen686
MRUOpen687
MRUOpen688
MRUOpen689
MRUOpen690
MRUOpen691
MRUOpen692
MRUOpen693
MRUOpen694
MRUOpen695
MRUOpen696
MRUOpen697
MRUOpen698
MRUOpen699
MRUOpen700
MRUOpen701
MRUOpen702
MRUOpen703
MRUOpen704
MRUOpen705
MRUOpen706
MRUOpen707
MRUOpen708
MRUOpen709
MRUOpen710
MRUOpen711
MRUOpen712
MRUOpen713
MRUOpen714
MRUOpen715
MRUOpen716
MRUOpen717
MRUOpen718
MRUOpen719
MRUOpen720
MRUOpen721
MRUOpen722
MRUOpen723
MRUOpen724
MRUOpen725
MRUOpen726
MRUOpen727
MRUOpen728
MRUOpen729
MRUOpen730
MRUOpen731
MRUOpen732
MRUOpen733
MRUOpen734
MRUOpen735
MRUOpen736
MRUOpen737
MRUOpen738
MRUOpen739
MRUOpen740
MRUOpen741
MRUOpen742
MRUOpen743
MRUOpen744
MRUOpen745
MRUOpen746
MRUOpen747
MRUOpen748
MRUOpen749
MRUOpen750
MRUOpen751
MRUOpen752
MRUOpen753
MRUOpen754
MRUOpen755
MRUOpen756
MRUOpen757
MRUOpen758
MRUOpen759
MRUOpen760
MRUOpen761
MRUOpen762
MRUOpen763
MRUOpen764
MRUOpen765
MRUOpen766
MRUOpen767
MRUOpen768
MRUOpen769
MRUOpen770
MRUOpen771
MRUOpen772
MRUOpen773
MRUOpen774
MRUOpen775
MRUOpen776
MRUOpen777
MRUOpen778
MRUOpen779
MRUOpen780
MRUOpen781
MRUOpen782
MRUOpen783
MRUOpen784
MRUOpen785
MRUOpen786
MRUOpen787
MRUOpen788
MRUOpen789
MRUOpen790
MRUOpen791
MRUOpen792
MRUOpen793
MRUOpen794
MRUOpen795
MRUOpen796
MRUOpen797
MRUOpen798
MRUOpen799
MRUOpen800
MRUOpen801
MRUOpen802
MRUOpen803
MRUOpen804
MRUOpen805
MRUOpen806
MRUOpen807
MRUOpen808
MRUOpen809
MRUOpen810
MRUOpen811
MRUOpen812
MRUOpen813
MRUOpen814
MRUOpen815
MRUOpen816
MRUOpen817
MRUOpen818
MRUOpen819
MRUOpen820
MRUOpen821
MRUOpen822
MRUOpen823
MRUOpen824
MRUOpen825
MRUOpen826
MRUOpen827
MRUOpen828
MRUOpen829
MRUOpen830
MRUOpen831
MRUOpen832
MRUOpen833
MRUOpen834
MRUOpen835
MRUOpen836
MRUOpen837
MRUOpen838
MRUOpen839
MRUOpen840
MRUOpen841
MRUOpen842
MRUOpen843
MRUOpen844
MRUOpen845
MRUOpen846
MRUOpen847
MRUOpen848
MRUOpen849
MRUOpen850
MRUOpen851
MRUOpen852
MRUOpen853
MRUOpen854
MRUOpen855
MRUOpen856
MRUOpen857
MRUOpen858
MRUOpen859
MRUOpen860
MRUOpen861
MRUOpen862
MRUOpen863
MRUOpen864
MRUOpen865
MRUOpen866
MRUOpen867
MRUOpen868
MRUOpen869
MRUOpen870
MRUOpen871
MRUOpen872
MRUOpen873
MRUOpen874
MRUOpen875
MRUOpen876
MRUOpen877
MRUOpen878
MRUOpen879
MRUOpen880
MRUOpen881
MRUOpen882
MRUOpen883
MRUOpen884
MRUOpen885
MRUOpen886
MRUOpen887
MRUOpen888
MRUOpen889
MRUOpen890
MRUOpen891
MRUOpen892
MRUOpen893
MRUOpen894
MRUOpen895
MRUOpen896
MRUOpen897
MRUOpen898
MRUOpen899
MRUOpen900
MRUOpen901
MRUOpen902
MRUOpen903
MRUOpen904
MRUOpen905
MRUOpen906
MRUOpen907
MRUOpen908
MRUOpen909
MRUOpen910
MRUOpen911
MRUOpen912
MRUOpen913
MRUOpen914
MRUOpen915
MRUOpen916
MRUOpen917
MRUOpen918
MRUOpen919
MRUOpen920
MRUOpen921
MRUOpen922
MRUOpen923
MRUOpen924
MRUOpen925
MRUOpen926
MRUOpen927
MRUOpen928
MRUOpen929
MRUOpen930
MRUOpen931
MRUOpen932
MRUOpen933
MRUOpen934
MRUOpen935
MRUOpen936
MRUOpen937
MRUOpen938
MRUOpen939
MRUOpen940
MRUOpen941
MRUOpen942
MRUOpen943
MRUOpen944
MRUOpen945
MRUOpen946
MRUOpen947
MRUOpen948
MRUOpen949
MRUOpen950
MRUOpen951
MRUOpen952
MRUOpen953
MRUOpen954
MRUOpen955
MRUOpen956
MRUOpen957
MRUOpen958
MRUOpen959
MRUOpen960
MRUOpen961
MRUOpen962
MRUOpen963
MRUOpen964
MRUOpen965
MRUOpen966
MRUOpen967
MRUOpen968
MRUOpen969
MRUOpen970
MRUOpen971
MRUOpen972
MRUOpen973
MRUOpen974
MRUOpen975
MRUOpen976
MRUOpen977
MRUOpen978
MRUOpen979
MRUOpen980
MRUOpen981
MRUOpen982
MRUOpen983
MRUOpen984
MRUOpen985
MRUOpen986
MRUOpen987
MRUOpen988
MRUOpen989
MRUOpen990
MRUOpen991
MRUOpen992
MRUOpen993
MRUOpen994
MRUOpen995
MRUOpen996
MRUOpen997
MRUOpen998
MRUOpen999
MRUOpen1000
```

Interpretation

MS Outlook data files found in these locations include Outlook PST and PST files. One should also check the Outlook Recent Outlook folder, which might be empty. The folder is named after the version of Outlook used. For more information on where to find the Outlook folder, see this handy chart:

<https://www.danware.com/papers/04/04012004/outlookfolders.htm>

⚠️ (Three later entries) The subkeys store file info from the Open/save dialog that specific

E-mail Attachments

Description

The email subkey estimates that 80% of email data is stored as attachments. Email subkeys only allow read. Attachments must be encoded with MIME/PEM format.

Location

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Outlook\Attachments
```

Index

```
IP
Application
Application\Microsoft\Outlook
Application\Microsoft\Outlook\Attachments
Application\Microsoft\Outlook\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments
Application\Microsoft\Outlook\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\Attachments\
```


Program Execution

- There are seven different methods of identifying program execution
 - UserAssist*
 - Last-Visited MRU*
 - RunMRU Start*
 - AppCompatCache
 - Jump Lists
 - Prefetch
 - RecentFileCache

Program Execution	UserAssist	Last-Visited MRU	RunMRU Start->Run	AppCompatCache	Jump Lists	Prefetch	Amacache.hve/RecentFileCache.bcf
	<p>Description GUI-based programs launched from the desktop are tracked in the launcher on a Windows system.</p> <p>Location %LOCALAPPDATA%\Microsoft\Windows\Recent\WinSxS\%username%\AppCompat\%date%\%time%\%user%\</p> <p>Interpretation: All values are RCE-1) Encoded <ul style="list-style-type: none"> GUID for XP 75048700 Active Desktop GUID for Win7/10 CEBFFC0D Executable File Execution F4E57C4B Shortcut File Execution </p>	<p>Description Tracks the specific executable used by an application to open the file document in the OpenRecentMRU key. In addition, the value also tracks the directory location for the last file that was accessed by the application.</p> <p>Example Notepad.exe was last run using the C:\WINDOWS\10\Desktop\ folder</p> <p>Location %LOCALAPPDATA%\Microsoft\Windows\Recent\WinSxS\%username%\AppCompat\%date%\%time%\%user%\</p> <p>Interpretation: The order in which the commands are executed is listed in the RunMRU list. The letters represent the order in which the commands were executed.</p>	<p>Description Whenever someone does a Start -> Run command, it will log the entry for the command they executed.</p> <p>Location %LOCALAPPDATA%\Microsoft\Windows\CurrentVersion\History\%date%\%time%\%user%\</p> <p>Interpretation: The order in which the commands are executed is listed in the RunMRU list. The letters represent the order in which the commands were executed.</p>	<p>Description <ul style="list-style-type: none"> Windows Application Compatibility Database is used by Windows to identify possible compatibility issues with applications. Tracks the executables file name, the exe, last modified time, and in Windows XP the last update time <p>Location %LOCALAPPDATA%\Microsoft\Windows\CurrentVersion\Compat\%date%\%time%\%user%\</p> <p>Interpretation: <ul style="list-style-type: none"> Windows XP contains at most 95 entries LastUpdateTime is updated when the files are executed Windows 7 contains at most 1,024 entries LastUpdateTime does not exist on Win7 systems </p> </p>	<p>Description <ul style="list-style-type: none"> The Windows 7 task bar 'Jump List' is engineered to allow users to "jump" or "access items they have. Customized or manually used file and device functionality cannot only include recent media files, it must also include recent tasks. The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the associated application. <p>Location %LOCALAPPDATA%\Microsoft\Windows\Recent\WinSxS\%username%\AppCompat\%date%\%time%\%user%\</p> <p>Interpretation: <ul style="list-style-type: none"> First time of execution of application. Creation Time = First time item added to the AppID file. Last time of execution of application will be open. Modification Time = Last time item added to the AppID file. List of Jump List IDs: http://www.sysinternals.com/wiki/index.php/Jump_List_IDs </p> </p>	<p>Description <ul style="list-style-type: none"> Increases performance of a system by pre-loading code of commonly used applications. Each application has a unique file and device functionality cannot only include recent media files, it must also include recent tasks. The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the associated application. Limited to 128 files on XP and Win7 Limited to 1024 files on Win8 (seamless/flush/p) <p>Location %LOCALAPPDATA%\Microsoft\Windows\Recent\WinSxS\%username%\AppCompat\%date%\%time%\%user%\</p> <p>Interpretation: <ul style="list-style-type: none"> Each pfw file includes last time of execution, number of times run, and device and file handles used by the program. Date/Time file by that name and path was first executed Creation Date of the file (1-10 seconds) Date/Time file by that name and path was last executed Embedded last time of execution of pf file Last modification date of pf file (1-10 seconds) Win7-10 will contain last 8 times of execution </p> </p>	<p>Description ProgramDataUpdater (a task located with the Application Experience Diagnostics) uses the registry file RecentFileCache.bcf to store data during process creation</p> <p>Location %LOCALAPPDATA%\Microsoft\Windows\Recent\WinSxS\%username%\AppCompat\%date%\%time%\%user%\</p> <p>Interpretation: <ul style="list-style-type: none"> RecentFileCache.bcf - Encodes RNTD and RLENAND and the program is executable not to the system The program executed on the system is the last ProgramDataUpdater task has been run Amacache - Key Amacache live from Vista/7/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100/101/102/103/104/105/106/107/108/109/110/111/112/113/114/115/116/117/118/119/120/121/122/123/124/125/126/127/128/129/130/131/132/133/134/135/136/137/138/139/140/141/142/143/144/145/146/147/148/149/150/151/152/153/154/155/156/157/158/159/160/161/162/163/164/165/166/167/168/169/170/171/172/173/174/175/176/177/178/179/180/181/182/183/184/185/186/187/188/189/190/191/192/193/194/195/196/197/198/199/200/201/202/203/204/205/206/207/208/209/210/211/212/213/214/215/216/217/218/219/220/221/222/223/224/225/226/227/228/229/230/231/232/233/234/235/236/237/238/239/240/241/242/243/244/245/246/247/248/249/250/251/252/253/254/255/256/257/258/259/260/261/262/263/264/265/266/267/268/269/270/271/272/273/274/275/276/277/278/279/280/281/282/283/284/285/286/287/288/289/290/291/292/293/294/295/296/297/298/299/300/301/302/303/304/305/306/307/308/309/310/311/312/313/314/315/316/317/318/319/320/321/322/323/324/325/326/327/328/329/330/331/332/333/334/335/336/337/338/339/340/341/342/343/344/345/346/347/348/349/350/351/352/353/354/355/356/357/358/359/360/361/362/363/364/365/366/367/368/369/370/371/372/373/374/375/376/377/378/379/380/381/382/383/384/385/386/387/388/389/390/391/392/393/394/395/396/397/398/399/400/401/402/403/404/405/406/407/408/409/410/411/412/413/414/415/416/417/418/419/420/421/422/423/424/425/426/427/428/429/430/431/432/433/434/435/436/437/438/439/440/441/442/443/444/445/446/447/448/449/450/451/452/453/454/455/456/457/458/459/460/461/462/463/464/465/466/467/468/469/470/471/472/473/474/475/476/477/478/479/480/481/482/483/484/485/486/487/488/489/490/491/492/493/494/495/496/497/498/499/500/501/502/503/504/505/506/507/508/509/510/511/512/513/514/515/516/517/518/519/520/521/522/523/524/525/526/527/528/529/530/531/532/533/534/535/536/537/538/539/540/541/542/543/544/545/546/547/548/549/550/551/552/553/554/555/556/557/558/559/560/561/562/563/564/565/566/567/568/569/570/571/572/573/574/575/576/57</p>

Program Execution – Prefetch

Prefetch

Description:

- Increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.
- Limited to 128 files on XP and Win7
- Limited to 1024 files on Win8
- (exename)-(hash).pf

Location:

WinXP/7/8/10

C:\Windows\Prefetch

Interpretation:

- Each .pf will include last time of execution, number of times run, and device and file handles used by the program
- Date/Time file by that name and path was first executed
 - Creation Date of .pf file (-10 seconds)
- Date/Time file by that name and path was last executed
 - Embedded last execution time of .pf file
 - Last modification date of .pf file (-10 seconds)
 - Win8-10 will contain last 8 times of execution

- Increases performance of a system by preloading commonly used applications
- Cache Manager monitors all files and directories for each application and maps them into a .pf file
- Proves application execution on a system
- Each prefetch file includes
 - ✓ Last execution time, number of times run, and program file handles
 - ✓ Date and time path was first executed
 - ✓ Creation Date of .pf file
 - ✓ Date and time file by that name and path was last executed

C:\Windows\Prefetch

File / Folder Opening

- In addition to some file and folder access artifacts that we have introduced in the Ranmore course, other methods include:
 - ✓ Open / Save MRU*
 - ✓ Last-Visted MRU*
 - ✓ Recent Files*
 - ✓ Shell Bags*
 - ✓ Prefetch
 - ✓ Link Files
 - ✓ Jump Lists
 - ✓ IE / Edge Browser Files

File/Folder Opening

File/Folder Opening	Open/Save MRU	Last-Visited MRU	Recent Files	Office Recent Files	Shell Bags	Shortcut (LNK) Files	Jump Lists	Prefetch	IE/Edge files://
Description In the simplest terms, this key tracks the files that have been opened or used within a Windows shell dialog box. The applets to be a data set, not only including what users have browsed, but also Explorer and Favorites, and also a directory of commonly used applications.	Description Tracks the specific executable used by an application to open the files documented in the Open/Save MRU. In addition, Explorer, which also tracks the directory location for the last file that was accessed by that application.	Description Registry Key that will track the last files and folders opened and is used to populate data in "Recent" menu of the Start menu.	Description MS Office programs will track their own Recent files to make it easier for users to retrieve the most recent last files they were editing.	Description When folders were accessed on the local machine, the network, or the Internet, Windows keeps a record of previously visited folders and subfolders. When certain folders were accessed.	Description - Shortcuts are automatically created by Windows - Recent items.	Description The Windows 7 task bar (Jump List) is engineered to allow users to "jump" to a specific file or folder with frequency or recently used quickly and easily. The functionality monitors when files are accessed, but must also include recent tasks.	Description - Increase performance of many system by pre-loading code objects and frequently used applications. Cache Manager monitors local and network resources for references for each application or process and maps them into the RAM of the system to know at application was executed on a system.	Description A little known fact about the IE History is that the information stored in the history files is not set or related to Internet browsing. The history also records local and network resources (via network paths) file access, such as an excellent means for determining which files and applications were accessed on the system, day by day.	
Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent	Location %USERPROFILE%\Recent
REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent
Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.	Interpretation RecentDocs - Overall view tracks the overall order of the last 100 files or folders opened. MRU lists keep track of the temporal order in which each file was opened. The last entry and modification time of this list will be the temporal order of the specific extension was opened.
REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime
REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime	REGEDIT HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecentDocs\RecentDocs\LastVisitedTime
Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.	Interpretation - The "****" key - This sub-key tracks the most recent file of any extension and only in the Explorer dialog.
Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.	Interpretation - JTF (These stores file info) from the Explorer dialog by specific extension.

File / Folder Opening – Link Files

- Links (LNK) are shortcuts automatically created by Windows for recent items and when opening local and remote data files
- Link files can provide valuable forensics information including:
 - ✓ LNK creation date
 - ✓ When LNK was last opened
 - ✓ LNK modification date
- LNK file data includes:
 - ✓ Target file MAC times
 - ✓ Volume Information
 - ✓ Network Share information
 - ✓ Original Location
 - ✓ System Name



C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent

File / Folder Opening – Jump Lists

Jump Lists

Description:

- The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items have frequently or recently used quickly and easily. This functionality cannot only include recent media files; it must also include recent tasks.
- The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the association application and embedded with LNK files in each stream.

Location:

Win7/8/10

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation:

- Using the Structured Storage Viewer, open up one of the AutomaticDestination jumplist files.
- Each one of these files is a separate LNK file. They are also stored numerically in order from the earliest one (usually 1) to the most recent (largest integer value).

- Jump Lists provide provides access to recently or frequently used items
- Jump lists includes both user files and recent tasks

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

- Data stored in this directory has unique files prepended with the associated application (AppID) and embedded file LNK
- Each LNK is stored numerically based on order of access, incremented from 1

File Knowledge

- The most common forensic artifacts relative to file knowledge:
 - ✓ WordWheelQuery
 - ✓ Last-Visited MRU*
 - ✓ Thumbscache
 - ✓ Recycle Bin*
 - ✓ Browser Files

Deleted File or File Knowledge	XP Search – ACMRU	Search – WordWheelQuery	Last-Visited MRU	Thumbs.db	Thumbscache	XP Recycle Bin	Win7/8/10 Recycle Bin	IE/Edge file://
	<p>Description: You can search for a wide range of information through the search assistant on a Windows XP machine. The search assistant will remember a user's search terms for filenames, computers, or words that are inside a file. This is an example of where you can find the "Search History" on the Windows system.</p> <p>Location: NTUSER.DAT\HKEY_CURRENT_USER\Software\Microsoft\Search\Assistant\History\History</p> <p>Interpretation: Keywords are added in Unicode and listed in temporal order in an MRU list.</p> <ul style="list-style-type: none"> • Search the Internet – 搜索结果=3001 • All or part of a document name – 搜索结果=5603 • A word or phrase in a file – 搜索结果=5604 • Printers, Computers and People – 搜索结果=5647 	<p>Description: Keywords searched for from the START menu bar on a Windows 7 machine.</p> <p>Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Recent\WordWheelQuery</p> <p>Interpretation: Keywords are added in Unicode and listed in temporal order in an MRU list.</p>	<p>Description: Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.</p> <p>Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Recent\LastVisitedMRU</p> <p>Interpretation: Keywords are added in Unicode and listed in temporal order in an MRU list.</p>	<p>Description: Hidden file in directory where images on machine exist stored in a similar thumbnail graphics. Thumbs.db catalogs pictures in a folder and stores a copy of the thumbnail even if the pictures were deleted.</p> <p>Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Recent\Thumbs.db</p> <p>Interpretation: Keywords are added in Unicode and listed in temporal order in an MRU list.</p>	<p>Description: Thumbnail of pictures, office documents, and folders exist in a database called the thumbscache. Each user will have their own database based on the thumbnail size viewed by the user (small, medium, large, and extra-large).</p> <p>Location: C:\Users\%USER%\AppData\Local\Microsoft\Windows\Thumbscache</p> <p>Interpretation: Keywords are added in Unicode and listed in temporal order in an MRU list.</p>	<p>Description: The recycle bin is a very important location on a Windows file system to understand. It can help you when accomplishing a forensic investigation, as every file that is deleted from a Windows recycle bin aware program is generally first put in the recycle bin.</p> <p>Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecycleBin</p> <p>Interpretation: Keywords are added in Unicode and listed in temporal order in an MRU list.</p>	<p>Description: The recycle bin is a very important location on a Windows file system to understand. It can help you when accomplishing a forensic investigation, as every file that is deleted from a Windows recycle bin aware program is generally first put in the recycle bin.</p> <p>Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RecycleBin</p> <p>Interpretation: Keywords are added in Unicode and listed in temporal order in an MRU list.</p>	<p>Description: A little-known fact about the IE History is that the information stored in the History file is not just related to Internet browsing. The history also records local and remote (via network shares) file access, giving us an excellent means for determining which files and applications were accessed on the system, day by day.</p> <p>Location: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History</p> <p>Interpretation: Keywords are added in Unicode and listed in temporal order in an MRU list.</p>

File Knowledge – WordWheelQuery

- Keywords searched for from the START menu bar on a Windows 7 / 8 / 10
- Keywords are added in Unicode and listed in temporal order in an MRUlist

Search – WordWheelQuery

Description:

Keywords searched for from the START menu bar on a Windows 7 machine.

Location:

Win7/8/10 NTUSER.DAT Hive
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Interpretation:

Keywords are added in Unicode and listed in temporal order in an MRUlist

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

File Knowledge – Browser Files

IE|Edge file://

Description:

A little-known fact about the IE History is that the information stored in the history files is not just related to Internet browsing. The history also records local and remote (via network shares) file access, giving us an excellent means for determining which files and applications were accessed on the system, day by day.

Location:

Internet Explorer:

IE6-7 %USERPROFILE%\LocalSettings\
History\History.IE5

IE8-9 %USERPROFILE%\AppData\Local\Microsoft\
WindowsHistory\History.IE5

IE10-11 %USERPROFILE%\AppData\Local\Microsoft\
Windows\WebCache\WebCacheV*.dat

Interpretation:

- Stored in index.dat as:
file:///C:/directory/filename.ext
- Does not mean file was opened in browser

- IE tracks both local and remote file access history, not just internet browsing history
- As a result, IE can provide history of when files and applications were accessed on a system along with timestamps
- IE 10 & 11 Locations

%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Physical Location

- There are four main ways to find forensics artifacts relative to the physical location of the system under investigation
 - ✓ Timezone
 - ✓ Network History
 - ✓ Cookies
 - ✓ Browser Search Terms

Physical Location	<h3>Timezone</h3> <p>Description: Identifies the current system time zone.</p> <p>Location: SYSTEM\Win SYSTEM\CurrentControlSet\Control\TimeZoneInformation</p> <p>Interpretation:</p> <ul style="list-style-type: none">• Time activity is incredibly useful for correlation of activity• Internal log files and date/timestamps will be based on the system time zone information• You might have other network devices and you will need to correlate information to the time zone information collected here.	<h3>Network History</h3> <p>Description:</p> <ul style="list-style-type: none">• Identify networks that the computer has been connected to• Networks could be wireless or wired• Identify domain name/intranet name• Identify SSID• Identify Gateway MAC Address <p>Location: WIN7\SOFTWARE\NHE</p> <ul style="list-style-type: none">• C:\WINDOWS\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged• C:\WINDOWS\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed• C:\WINDOWS\Microsoft\Windows NT\CurrentVersion\NetworkList\UI\Cache <p>Interpretation:</p> <ul style="list-style-type: none">• Identifying intranets and networks that a computer has connected to is incredibly important• Not only can you determine the intranet name, you can determine the last time the network was connected to it based on the last write time of the key• This will also list any networks that have been connected to via a VPN• MAC Address of SSID for Gateway could be physically triangulated	<h3>Cookies</h3> <p>Description: Cookies give insight into what websites have been visited and what activities may have taken place there.</p> <p>Location:</p> <p>Internet Explorer</p> <ul style="list-style-type: none">• %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies• %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies• %USERPROFILE%\AppData\Local\Microsoft\Windows\InternetCookies <p>Firefox</p> <ul style="list-style-type: none">• %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<random text>\.default\cookies.sqlite• %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>\.default\cookies.sqlite <p>Chrome</p> <ul style="list-style-type: none">• %USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\Local Storage <p>WIN7\SOFTWARE\NHE\Google\Chrome\User Data\Default\Local Storage</p>	<h3>Browser Search Terms</h3> <p>Description: Records websites visited by date and time. Details stored for each local user account. Records number of times visited (frequency). Also tracks access of local system files. This will also include the website history of search terms in search engines.</p> <p>Location:</p> <p>Internet Explorer</p> <ul style="list-style-type: none">• %USERPROFILE%\Local Settings\History\History.IBS• %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IBS• %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV9.dat <p>Firefox</p> <ul style="list-style-type: none">• %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<random text>\.default\places.sqlite <p>WIN7\SOFTWARE\NHE\Google\Chrome\User Data\Default\places.sqlite</p>
-------------------	--	---	---	---

Physical Location – Cookies

- Cookies identify viewed websites and track network details including IP, date / time, and time zone
- IE, Firefox, and Chrome and each have specific cookie storage locations
 - ✓ IE 11 Cookies

%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies

- ✓ Firefox Cookies

%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite

- ✓ Chrome Cookies

%USERPROFILE%\AppData\Local\Google\Chrome\UserData\Default\Local Storage



External Device / USB Usage

- Windows provides seven artifacts for the forensic analysis of externally connected devices
 - ✓ Key Identification
 - ✓ First / Last Device Connection Times*
 - ✓ User – USB Identification
 - ✓ Device VSN*
 - ✓ Device Drive Letter*
 - ✓ LNK File
 - ✓ PnP Events

External Device/USB Usage	Key Identification	First/Last Times	User	Volume Serial Number	Drive Letter & Volume Name	Shortcut (LNK) Files
	Description: Track USB devices plugged into a machine. Location: • C:\SYSTEM\CurrentControlSet\Enum\USB • C:\SYSTEM\CurrentControlSet\Enum\USB Interpretation: • Identify vendor/product, and version of a USB device plugged into a machine. • Identify a unique USB device plugged into the machine. • Determine the time a device was plugged into the machine. • Devices that do not have a unique serial number will have an "0" in the second character of the serial number.	Description: Determine temporal usage of specific USB devices connected to a Windows Machine. Location: First/Last • P:\Program Log File Logs • C:\Windows\logsetupapi.log • C:\Windows\Log\logsetupapi.der.log Interpretation: • Search for Device Serial Number • Log file times are set to local time zone Locations: First.Last\enrtime\Time(Win/No/Any) %SystemRoot%\System32\enum\usb\usbdev\Vendor_Version\Device_SerialNumber\SerialNumber	Description: Find User that used the Unique USB Device. Location: • Look for GUID from C:\SYSTEM\MountedDevices • HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\UserPointedAt Interpretation: This GUID will be used next to identify the user that plugged in the device. The last write time of the key also corresponds to the last time the device was plugged into the machine by that user. The number will be referenced in the user's personal mountpoints key in the NTUSER.DAT file.	Description: Discover the Volume Serial Number of the Releystem Partition on the USB. (NOTE: This is not the USB Unique Serial Number which is hardcoded into the device firmware.) Location: • SYSTEM\Microsoft\WindowsNT\CurrentVersion\mountpoints • Use Volume Name and Unique Serial Number to find last integer number in link • Convert Decimal Serial Number to Hex Serial Number Interpretation: • Knowing both the Volume Serial Number and the Volume Name, you can concatenate the data across SHORTCUT FILE (LNK) names and the RECENTDOCX key. • The Shortcut File (LNK) contains the Volume Serial Number and Name. • RecentDoc Registry Key in most cases, will contain the volume name when the USB device is opened via Explorer	Description: Discover the first drive letter of the USB Device when it was plugged into the machine. Location: • Find PercentIDtoPaths • SYSTEM\CurrentControlSet\Enum\USBDEVOR • Using PercentIDtoPaths Discover Last Mount Point • SYSTEM\MountedDevices Win7/8/10: • SYSTEM\MountedDevices Portable Devices\Devices • SYSTEM\MountedDevices • Examining Drive Letters looking at Value Data Looking for Serial Number Interpretation: Identify the USB device that was last mapped to a specific drive letter. This technique only works for the last drive mapped. It does not contain historical records of every drive letter mapped to a removable drive.	Description: Shortcut files automatically created by Windows • Recent Items • Open local and remote data files and documents will generate a shortcut file (.lnk) Locations: • %SystemRoot%\StartMenu • %SystemRoot%\AppData\Roaming\Microsoft\Windows\Recent\CustomizedIconsList\AppData\Roaming\Microsoft\Office\Recent Interpretation: • Creation Time of file that name was first opened • Date/Time Date of Shortcut (LNK) File • Date/Time file of that name was last information • Last Modification Date of Shortcut (LNK) File • LNKTypeTag file (Internal LNK file format) • Modified Access, and Creation times of the target file (Name Information (Name, Type, Serial Number)) • Network Share Information • Original Location • Name of System Description: When a Plug and Play driver install is attempted, the service will log an ID 20001 event and provide a Status within the event. It is important to note that this event will trigger for any Plug and Play device, including but not limited to USB, Firewire, and PCMCIA devices. Locations: System file Win7/8/10 systemroot\System32\wininit\Logs\System.txt Interpretation: • Event ID 20001 – Plug and Play driver install attempted • Event ID 20001 • Timestamp • Device information • Device serial number • Status (0 = no error)

External Device / USB Usage – Key Identification

Key Identification

Description:

Track USB devices plugged into a machine.

Location:

- `SYSTEM\CurrentControlSet\Enum\USBSTOR`
- `SYSTEM\CurrentControlSet\Enum\USB`

Interpretation:

- Identify vendor, product, and version of a USB device plugged into a machine
- Identify a unique USB device plugged into the machine
- Determine the time a device was plugged into the machine
- Devices that do not have a unique serial number will have an "&" in the second character of the serial number.

Track USB devices plugged into a specific system
Identify vendor, product, and version of a USB device plugged into a machine

Determine the time a device was plugged into the machine

Devices that do not have a unique serial number will have an "&" in the second character of the serial number.

Account Usage

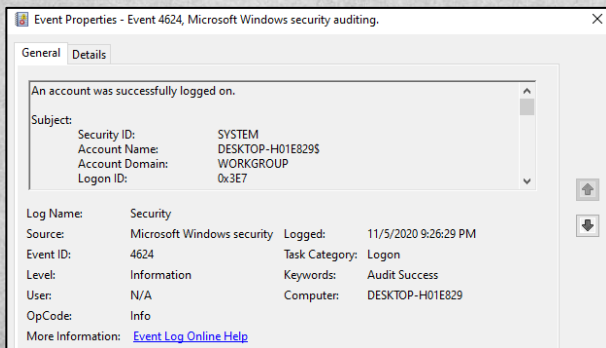
- Windows provides eight artifacts relative to account usage that can be identified through event logs and associated event ID's:
 - ✓ Last Login
 - ✓ Last Password Change
 - ✓ Success / Fail Logons
 - ✓ Logon Types
 - ✓ RDP Usage
 - ✓ Service Events
 - ✓ Scheduled Tasks
 - ✓ Authentication Events

Account Usage

Last Login	Last Password Change	Success/Fail Logons	Logon Types	RDP Usage	Services Events	Scheduled Tasks	Authentication Events																												
<p>Description:</p> <p>Lists the local accounts of the system and their equivalent security identifiers.</p> <p>Location:</p> <ul style="list-style-type: none">• C:\Windows\System32\config\SAM• SAM\Domains\Account\Users <p>Interpretation:</p> <ul style="list-style-type: none">• Only the last login time will be stored in the registry key	<p>Description:</p> <p>Lists the last time the password of a specific local user has been changed.</p> <p>Location:</p> <ul style="list-style-type: none">• C:\Windows\System32\config\SAM• SAM\Domains\Account\Users <p>Interpretation:</p> <ul style="list-style-type: none">• Only the last password change time will be stored in the registry key	<p>Description:</p> <p>Determine which accounts have been used for attempted logons. Track account usage for known compromised accounts.</p> <p>Location:</p> <p>HKEY_LOCAL_MACHINE\System\currentControlSet\Windows\logonui\Security.evtx</p> <p>Interpretation:</p> <ul style="list-style-type: none">• Win7/8/10 – Interpretation• 4624 – Successful Logon• 4625 – Failed Logon• 4634 / 4647 – Successful Logoff• 4648 – Logon using explicit credentials (Remote)• 4672 – Account logon with supervisor rights (Administrator)• 4720 – An account was created	<p>Description:</p> <p>Logon Events can give us very specific information regarding the nature of account authentications on a system. I was keen to find out how to decipher the data that we find. In addition to telling us the date, time, username, hostname, and successful/failure status of a logon, Logon Events also enables us to determine by exactly what means a logon was attempted.</p> <p>Location:</p> <p>HKEY_LOCAL_MACHINE\System\currentControlSet\Windows\logonui\Security.evtx</p> <p>Interpretation:</p> <table><thead><tr><th>Logon Type</th><th>Explanation</th></tr></thead><tbody><tr><td>1</td><td>Logon via console</td></tr><tr><td>2</td><td>Network Logon</td></tr><tr><td>3</td><td>Batch Logon</td></tr><tr><td>4</td><td>Windows Service Logon</td></tr><tr><td>5</td><td>Credentials used to unlock screen</td></tr><tr><td>6</td><td>Network logon sending credential (cleartext)</td></tr><tr><td>7</td><td>Different credentials used than logged on user</td></tr><tr><td>8</td><td>Remote interactive logon (RDP)</td></tr><tr><td>9</td><td>Cached credentials used to logon</td></tr><tr><td>10</td><td>Cached remote interactive (similar to Type 10)</td></tr><tr><td>11</td><td>Cached unlock (similar to Type 7)</td></tr><tr><td>12</td><td></td></tr><tr><td>13</td><td></td></tr></tbody></table>	Logon Type	Explanation	1	Logon via console	2	Network Logon	3	Batch Logon	4	Windows Service Logon	5	Credentials used to unlock screen	6	Network logon sending credential (cleartext)	7	Different credentials used than logged on user	8	Remote interactive logon (RDP)	9	Cached credentials used to logon	10	Cached remote interactive (similar to Type 10)	11	Cached unlock (similar to Type 7)	12		13		<p>Description:</p> <p>Track Remote Desktop Protocol logons to target machines.</p> <p>Location: Security.evtx</p> <p>HKEY_LOCAL_MACHINE\System\currentControlSet\Windows\logonui\Security.evtx</p> <p>Interpretations:</p> <ul style="list-style-type: none">• Win7/8/10 – Interpretation• Event ID 4778 – Session Connected/Reconnected• Event ID 4779 – Session Disconnected• Event log provides hostname and IP address of remote machine making the connection• On workstations you will often see current console session disconnected (4779) followed by RDP connection (4778)	<p>Description:</p> <p>Identify and audit services running at boot time</p> <ul style="list-style-type: none">• Review services started or stopped around the time of a suspected compromise <p>Location:</p> <p>All Event IDs reference the System Log</p> <p>7034 – Service crashed unexpectedly</p> <p>7035 – Service sent a Start/Stop control</p> <p>7036 – Service started or stopped</p> <p>7040 – Start type changed (Boot On Request Disabled)</p> <p>7045 – A service was installed on the system (Win2008R2+)</p> <p>4697 – A service was installed on the system (from Security log)</p> <p>Interpretation:</p> <ul style="list-style-type: none">• All Event IDs except 4697 reference the System Log Services• A large amount of malware and worms in the wild utilise Services• Services started on boot illustrate persistence (desirable in malware)• Services can crash due to attacks like process injection	<p>Description:</p> <p>Identify and audit scheduled tasks</p> <p>Location:</p> <p>System\currentControlSet\Windows\logonui\Security.evtx</p> <p>System\currentControlSet\Windows\logonui\Microsoft-Windows-TaskScheduler\TaskScheduler\Security.evtx</p> <p>Interpretations:</p> <ul style="list-style-type: none">• 105 / 4698 – Scheduled task created (Task Scheduler\Security log)• 140 / 4702 – Scheduled task updated (Task Scheduler\Security log)• 141 / 4699 – Scheduled task deleted (Task Scheduler\Security log)• 200 / 201 – Scheduled task executed/completed (Task Scheduler log)• 4700 / 4701 – Scheduled task enabled/disabled (Security log) <p>Investigative Notes</p> <ul style="list-style-type: none">• Scheduled tasks can be executed both locally and remotely• Remotely scheduled tasks also cause Logon ID 4624• Type 3 events	<p>Description:</p> <p>Authentication mechanisms</p> <p>Location:</p> <p>Local Account/Workgroup = on workstation</p> <p>Domain/Active Directory = on domain controller</p> <p>HKEY_LOCAL_MACHINE\System\currentControlSet\Windows\logonui\Security.evtx</p> <p>Interpretations:</p> <p>Event ID Codes (NTLM protocol)</p> <ul style="list-style-type: none">• 4776: Successful account authentication <p>Event ID Codes (Kerberos protocol)</p> <ul style="list-style-type: none">• 4788: Ticket Granting Ticket was granted (successful logon)• 4789: Service Ticket requested (access to server resource)• 4771: Pre-authentication failed (failed logon)
Logon Type	Explanation																																		
1	Logon via console																																		
2	Network Logon																																		
3	Batch Logon																																		
4	Windows Service Logon																																		
5	Credentials used to unlock screen																																		
6	Network logon sending credential (cleartext)																																		
7	Different credentials used than logged on user																																		
8	Remote interactive logon (RDP)																																		
9	Cached credentials used to logon																																		
10	Cached remote interactive (similar to Type 10)																																		
11	Cached unlock (similar to Type 7)																																		
12																																			
13																																			

Account Usage – Logons

- Windows event logs provide audit information for successful and unsuccessful logins
- Some of the more common logon related event ID's include:
 - ✓ Successful Logon – 4624
 - ✓ Failed Logon – 4625
 - ✓ Successful Logon – 4634 / 4647
 - ✓ Account Created – 4720



Success/Fail Logons

Description:

Determine which accounts have been used for attempted logons. Track account usage for known compromised accounts.

Location:

Win7/8/10

%system root%\System32\winevt\logs\Security.evtx

Interpretation:

- Win7/8/10 – Interpretation
- 4624 – Successful Logon
- 4625 – Failed Logon
- 4634 | 4647 – Successful Logoff
- 4648 – Logon using explicit credentials (Runas)
- 4672 – Account logon with superuser rights (Administrator)
- 4720 – An account was created

%system root%\System32\winevt\logs

Account Usage – RDP Usage

RDP Usage

Description:

Track Remote Desktop Protocol logons to target machines.

Location: Security Log

Win7/8/10

%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Interpretation:

- Win7/8/10 - Interpretation
 - Event ID 4778 – Session Connected/Reconnected
 - Event ID 4779 – Session Disconnected
- Event log provides hostname and IP address of remote machine making the connection
- On workstations you will often see current console session disconnected (4779) followed by RDP connection (4778)

- Remote Desktop Protocol allows remote connection and graphical access to Windows systems
- Event log ID's related to RDP connections:
 - ✓ Session Connected or Reconnected – 4778
 - ✓ Session Disconnected – 4779
- Event logs will contain additional networking information
 - ✓ Remote IP Address
 - ✓ Hostname

%system root%\System32\winevt\logs\Security.evtx

Browser Usage

- There are six different artifacts relative to browser account usage:
 - ✓ History
 - ✓ Cookies
 - ✓ Cache
 - ✓ Session Restore
 - ✓ Flash and Super Cookies
 - ✓ Google Analytics Cookies

Browser Usage					
History	Cookies	Cache	Session Restore	Flash & Super Cookies	Google Analytics Cookies
<p>Description: Records websites visited by date and time. Details stored for each local user account. Records number of times visited (frequency). Also tracks access of local system files.</p> <p>Location: Internet Explorer -H9-4 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-9 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-11 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125</p> <p>Firefox -H9-1 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite -H9-10 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite</p> <p>Chrome -H9-1 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History -H9-10 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History</p>	<p>Description: Cookies give insight into what websites have been visited and what activities may have taken place there.</p> <p>Location: Internet Explorer -H9-4 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-9 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-11 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125</p> <p>Firefox -H9-1 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite -H9-10 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite</p> <p>Chrome -H9-1 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History -H9-10 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History</p>	<p>Description: The cache is where web page components can be stored locally to speed up subsequent visits</p> <p>Location: Internet Explorer -H9-4 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-9 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-11 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125</p> <p>Firefox -H9-1 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite -H9-10 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite</p> <p>Chrome -H9-1 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History -H9-10 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History</p>	<p>Description: Automatic Crash Recovery features built into the browser.</p> <p>Location: Internet Explorer -H9-4 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-9 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-11 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125</p> <p>Firefox -H9-1 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite -H9-10 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite</p> <p>Chrome -H9-1 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History -H9-10 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History</p>	<p>Description: Local Stored Objects (LSOs), or Flash Cookies, have become ubiquitous on most systems due to the extremely high penetration of Flash applications across the Internet. They tend to be much more persistent because they do not expire, and there is no built-in mechanism within the browser to remove them. In fact, many sites have begun using LSOs for their tracking mechanisms because they rarely get cleared like traditional cookies.</p> <p>Location: -H9-1 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-9 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125 -H9-11 HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\History\History.125</p> <p>Firefox -H9-1 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite -H9-10 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite</p> <p>Chrome -H9-1 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History -H9-10 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History</p>	<p>Description: Google Analytics (GA) has developed an extremely sophisticated methodology for tracking site visits, user activity and paid search. Since GA is largely free, it has a commanding share of the market, estimated at over 80% of sites using traffic analysis and over 50% of all sites.</p> <p>Location: -H9-1 HKEYCURRENTUSER\Software\Google\Analytics\History\History.125 -H9-9 HKEYCURRENTUSER\Software\Google\Analytics\History\History.125 -H9-11 HKEYCURRENTUSER\Software\Google\Analytics\History\History.125</p> <p>Firefox -H9-1 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite -H9-10 HKEYCURRENTUSER\Software\Mozilla\Firefox\Profiles*\chrome\tabs\default\places.sqlite</p> <p>Chrome -H9-1 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History -H9-10 HKEYCURRENTUSER\Software\Google\Chrome\User Data\Default\History</p>

Timeline Analysis Tools

- With a knowledge of the different artifacts and their associated storage paths within Windows, we can now introduce the types of tools that can assist with providing a chronological listing of events
- Keep in mind that different artifacts are going to format time related information in different ways, so it will be necessary to parse files in different formats
- A few examples of some commercial and open-source log parsing and aggregation tools include:
 - ✓ LogStash
 - ✓ Splunk
 - ✓ Log2Timeline / Plaso
 - ✓ Timesketch

Log2Timeline / Plaso

- Plaso is a Python-based backend engine for Log2Timeline which is used to extract timestamps and aggregate results
- Some capabilities available when using these two tools:
 - ✓ Parsing Engines
 - ✓ Plug-Ins
 - ✓ Tagged Events

date	time	MACB	sourcetype	type	short
39649	0:06:15	MACB	Email PST	Email Read	Message 134: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MACB	XP Prefetch	Last run	EXCELEXE-1C75F8D6.pf: EXCELEXE was executed
7/20/2008	1:27:40	.AC.	NTFS \$MFT	\$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCELEXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launch	UEFI: RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCELEXE
7/20/2008	1:28:03	.CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:043	MACB	NTFS \$MFT	\$SI [MACB] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/Desktop.LNK
7/20/2008	1:28:03	MACB	FileExts key	Extension Change	File extension .xls opened by EXCELEXE
7/20/2008	1:28:03	MACB	NTFS \$MFT	\$SI [MACB] time	C:/windows/system32/winsvchost.exe
7/20/2008	1:28:03		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Jean
7/20/2008	1:27:40		Memory Process	Process Started	winsvchost.exe[1556][1032][0x02476768
7/20/2008	1:27:40		Memory Socket	Socket Opened	4[134.182.111.82:443][Protocol: 6 (TCP)][0x8162de98][]
7/20/2008	1:27:40		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCELEXE was executed
7/20/2008	1:28:03	.CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:03	.A..	Shortcut LNK	Access	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:04	MAC.	NTFS \$MFT	\$SI [MAC.] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
7/20/2008	1:28:04	.C..	NTFS \$MFT	\$SI [.C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IES/MSHist01200807202008
7/20/2008	1:28:04	.C..	NTFS \$MFT	\$SI [.C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IES/MSHist01200807202008
7/20/2008	1:28:04	MACB	RecentDocs key	File opened	Recently opened file of extension: .xls - value: m57biz.xls

Log2Timeline Installation

- We will use Log2Timeline to aggregate our Windows artifacts
- Installation:
 - ✓ <https://plaso.readthedocs.io/en/latest/sources/user/Ubuntu-Packaged-Release.html>
 - ✓ `sudo add-apt-repository ppa:gift/stable`
 - ✓ `sudo apt-get update`
 - ✓ `sudo apt-get install plaso-tools`