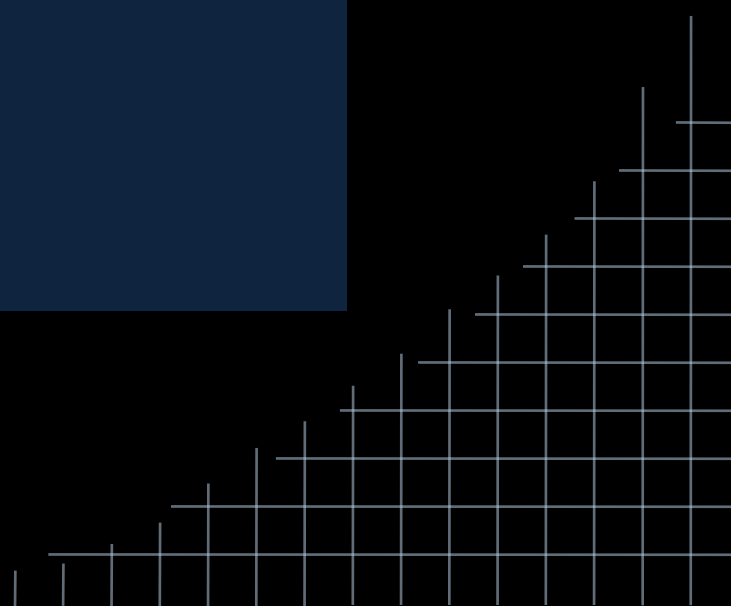




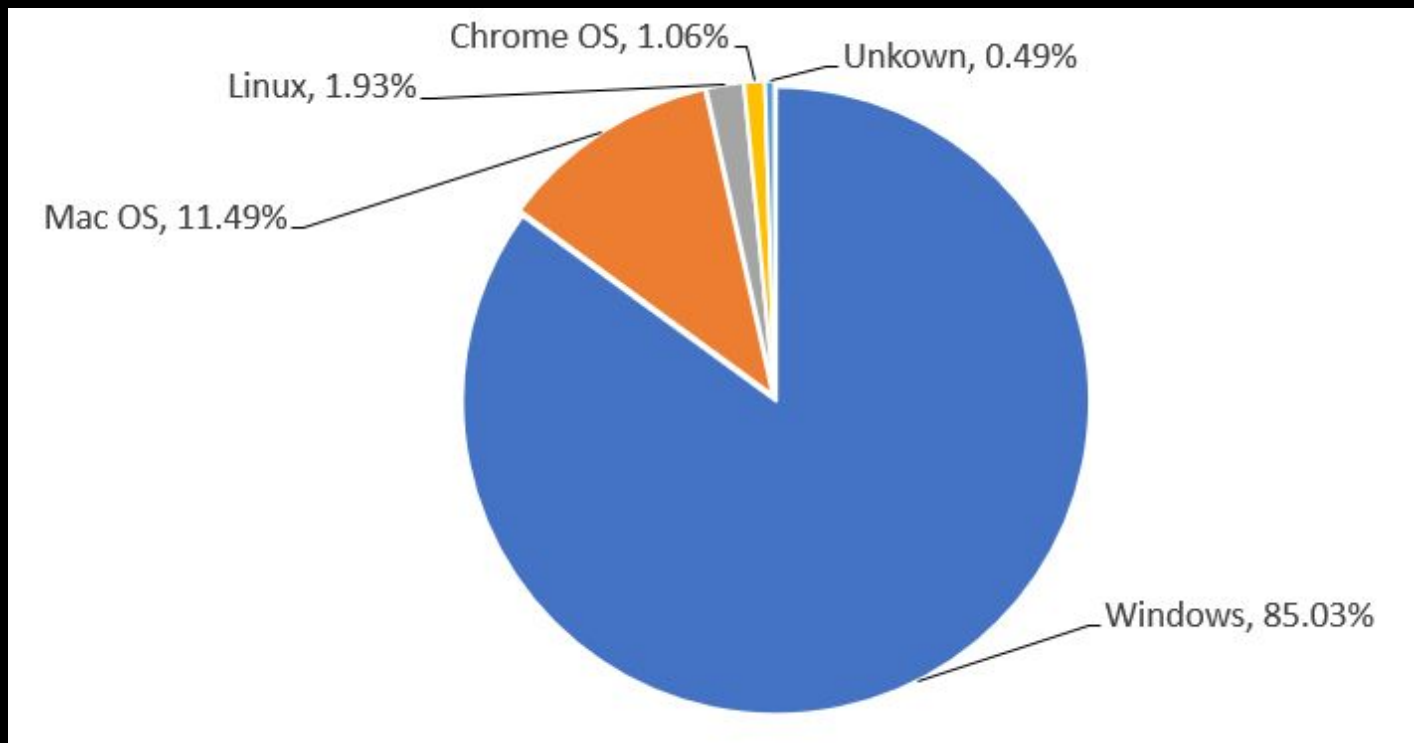
FORFUN

Week 3 Windows Forensics
Soraya Harding & Rahim Taheri



Why Windows Forensics?

- Windows Operating Systems are the most popular OS in the market (i.e. more than 85% of the market share)



Source:

<https://www.netmarketshare.com/operating-system-market-share.aspx?>

Windows Artefacts

- What kind of artefacts can you obtain from a suspect's hard drive (assuming installed with Windows OS) if you were the forensic investigator?

Interesting Folders

- C:\users\%username%\[Desktop, Downloads, Pictures]
- C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Recent
- C:\Users\%username%\AppData\Roaming\Microsoft\Office\Recent
- C:\Users\%username%\AppData\Local\Microsoft\Windows\Explorer
- C:\program files
- C:\program files (x86)
- C:\Windows\Prefetch
- C:\windows\System32\spool\PRINTERS
- C:\Windows\System32\winevt\Logs

Recycle Bin Artefacts

C:\ Command Prompt

```
C:\RECYCLER>cd S-1-5-21-839522115-1677128483-854245398-1003
```

```
C:\RECYCLER\S-1-5-21-839522115-1677128483-854245398-1003>dir /a
```

Volume in drive C has no label.

Volume Serial Number is 70C3-36D9

Directory of C:\RECYCLER\S-1-5-21-839522115-1677128483-854245398-1003

01/26/2014	08:34 PM	<DIR>	.
01/26/2014	08:34 PM	<DIR>	..
05/12/2013	05:55 PM		0 Dc1.exe
05/12/2013	05:46 PM		6,144 Dc2.exe
05/12/2013	06:06 PM		73,802 Dc3.exe
05/12/2013	06:33 PM		0 Dc4.exe
02/12/2013	03:14 PM		276,829,524 Dc5.7z
01/11/2013	12:47 PM	<DIR>	Dc6
05/13/2013	10:24 PM		609,410 Dc7.vbs
05/13/2013	08:32 PM		73,802 Dc8.exe
05/29/2013	05:01 PM		694 Dc9.lnk
05/12/2013	05:55 PM		65 desktop.ini
01/26/2014	08:34 PM		7,220 INF02
		10 File(s)	277,600,661 bytes
		3 Dir(s)	6,040,461,312 bytes free

```
C:\RECYCLER\S-1-5-21-839522115-1677128483-854245398-1003>_
```

Recycle Bin Artefacts

Administrator: Command Prompt

```
C:\$Recycle.Bin\S-1-5-21-579868786-2669328126-3886333572-221256>dir /a
Volume in drive C is OSDisk
Volume Serial Number is 847C-9C5E

Directory of C:\$Recycle.Bin\S-1-5-21-579868786-2669328126-3886333572-221256

24/10/2018  09:50    <DIR>          .
24/10/2018  09:50    <DIR>          ..
24/10/2018  09:26             114 $IJ47YIC.txt
19/10/2018  12:02           1,849 $RJ47YIC.txt
15/05/2018  15:53             129 desktop.ini
               3 File(s)                2,092 bytes
               2 Dir(s)  160,175,644,672 bytes free

C:\$Recycle.Bin\S-1-5-21-579868786-2669328126-3886333572-221256>
```



Thumbs.db

Thumbcache Viewer

File Edit View Tools Help

#	Filename	Cache Entr...	Cache ...	Data Offset	Data Si...	Data Checksum	Header Checksum	Cache Entry Hash
68	1884870179...	17074850 B	54 KB	17074930 B				1884870179612f10
69	451242086f...	6177850 B	51 KB	6177930 B				451242086fb8fee6
70	4512428e2d...	8090063 B	51 KB	8090143 B				4512428e2d2e439e
71	37470da89a...	55982212 B	50 KB	55982292 B				37470da89aedf0ac
72	7cb47ddb...	31481065 B	50 KB	31481145 B				7cb47ddb51100f
73	53ac8901b3...	649718 B	50 KB	649798 B				53ac8901b321bcb2
74	53ac892330...	1706347 B	50 KB	1706427 B				53ac892330104f07
75	2012af324a...	26512878 B	50 KB	26512958 B				2012af324a17d561
76	188484bda1...	22244559 B	50 KB	22244639 B				188484bda13a5c86
77	83c45ca2c3...	16135570 B	50 KB	16135650 B				83c45ca2c396585e
78	bc60820792...	26822207 B	48 KB	26822287 B				bc60820792aa7939
79	abcc7323da...	42033943 B	48 KB	42034023 B				abcc7323da890e77
80	a1c0097cd4...	24373263 B	48 KB	24373343 B				a1c0097cd48d1507
81	a1c0ff171d4...	20678496 B	47 KB	20678576 B	47 KB	86061f6cd3669...	ba771d3002a82a0a	a1c0ff171d417d70
82	df3a93c147...	8244143 B	47 KB	8244223 B	47 KB	4ff204ae44e5e8...	bb63abce96923922	df3a93c147250e5f
83	bc60821facf...	26871813 B	47 KB	26871893 B	47 KB	16f35d43dcbd9...	9165505fa58b0a54	bc60821facf92d61

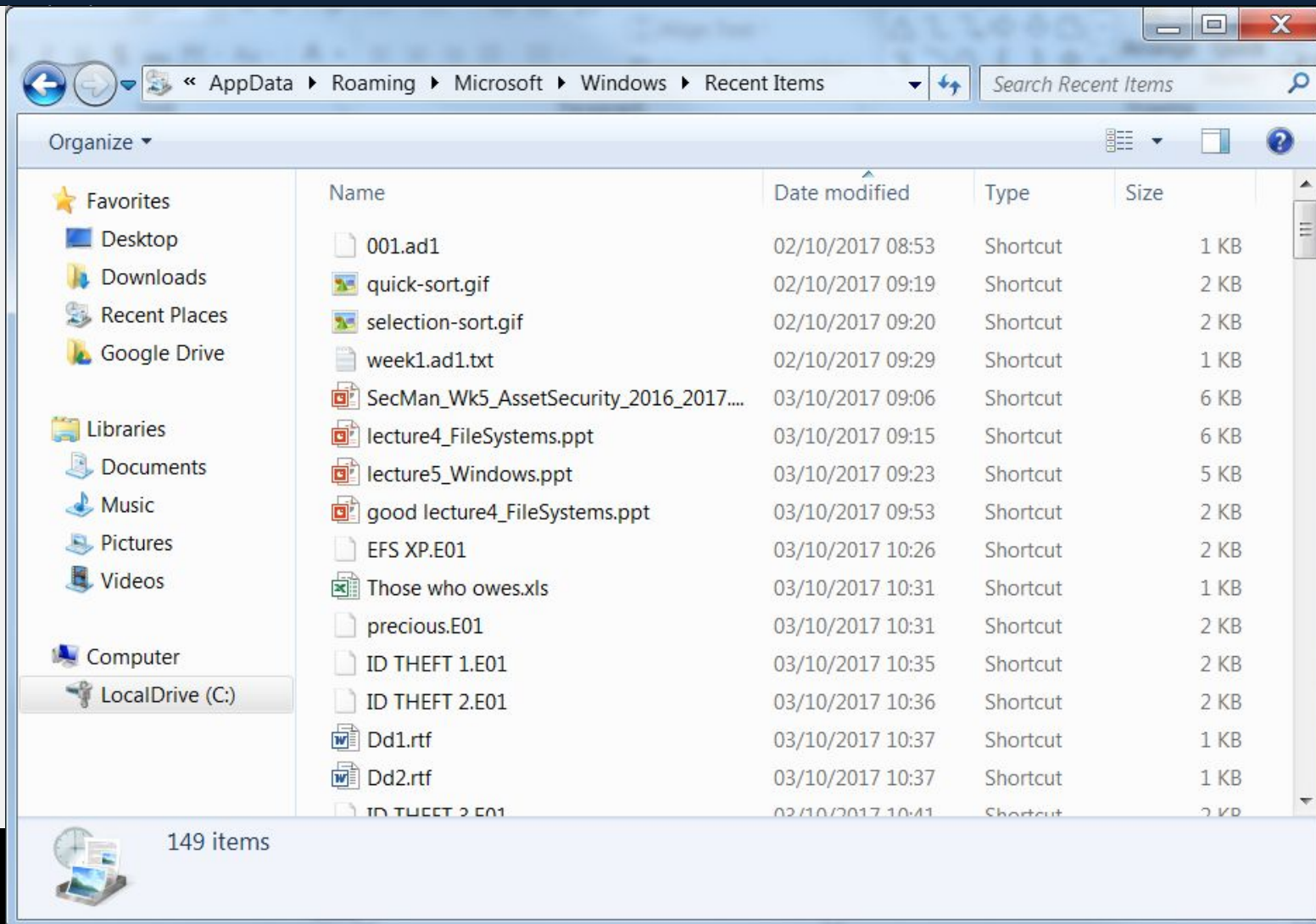
df3a93c147250e5f.p...



Link Files

- Link files are shortcuts for local or network programs, files, folders, computers (.lnk) or Web addresses (.url)
- Information that can be found within .lnk files
 - Original path of the target file.
 - Timestamp of both the target and the “.lnk” file (Created, Modified, Accessed).
 - File Attributes (System, Hidden...etc.)
 - Details about the disk.
 - Remote or local execution.
 - MAC address of the machines.

Link Files

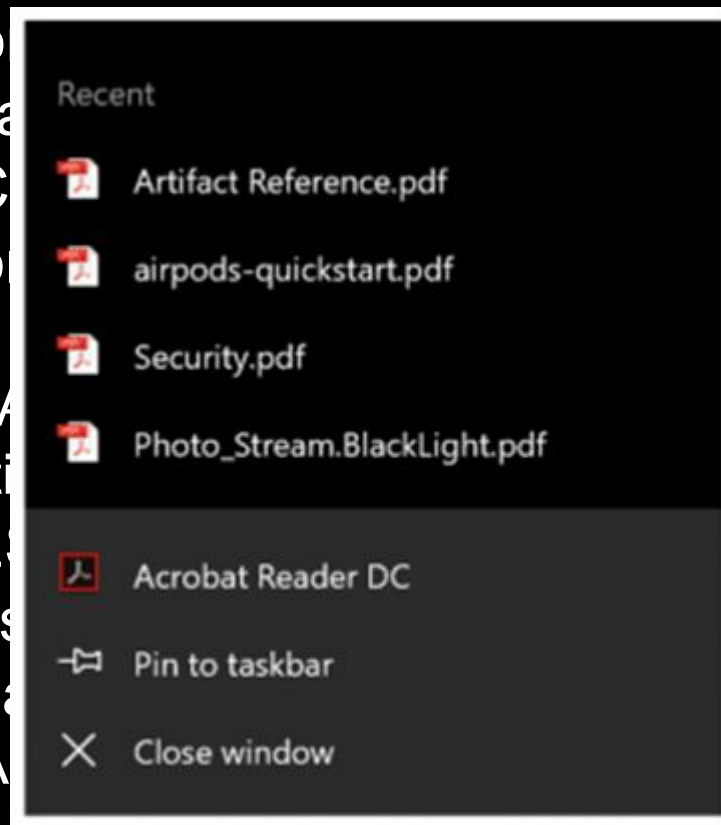


Jump Lists

- Jump Lists are a windows feature introduced with Windows 7. They contain information about recently accessed applications and files.
- AUTOMATICDESTINATIONS-MS: Which are jump lists created automatically when the user opens a file or an application;
 - C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- CUSTOMDESTINATIONS-MS: As their name indicated these are custom made jump lists, created when the user pins a file or an application
 - C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

Jump Lists

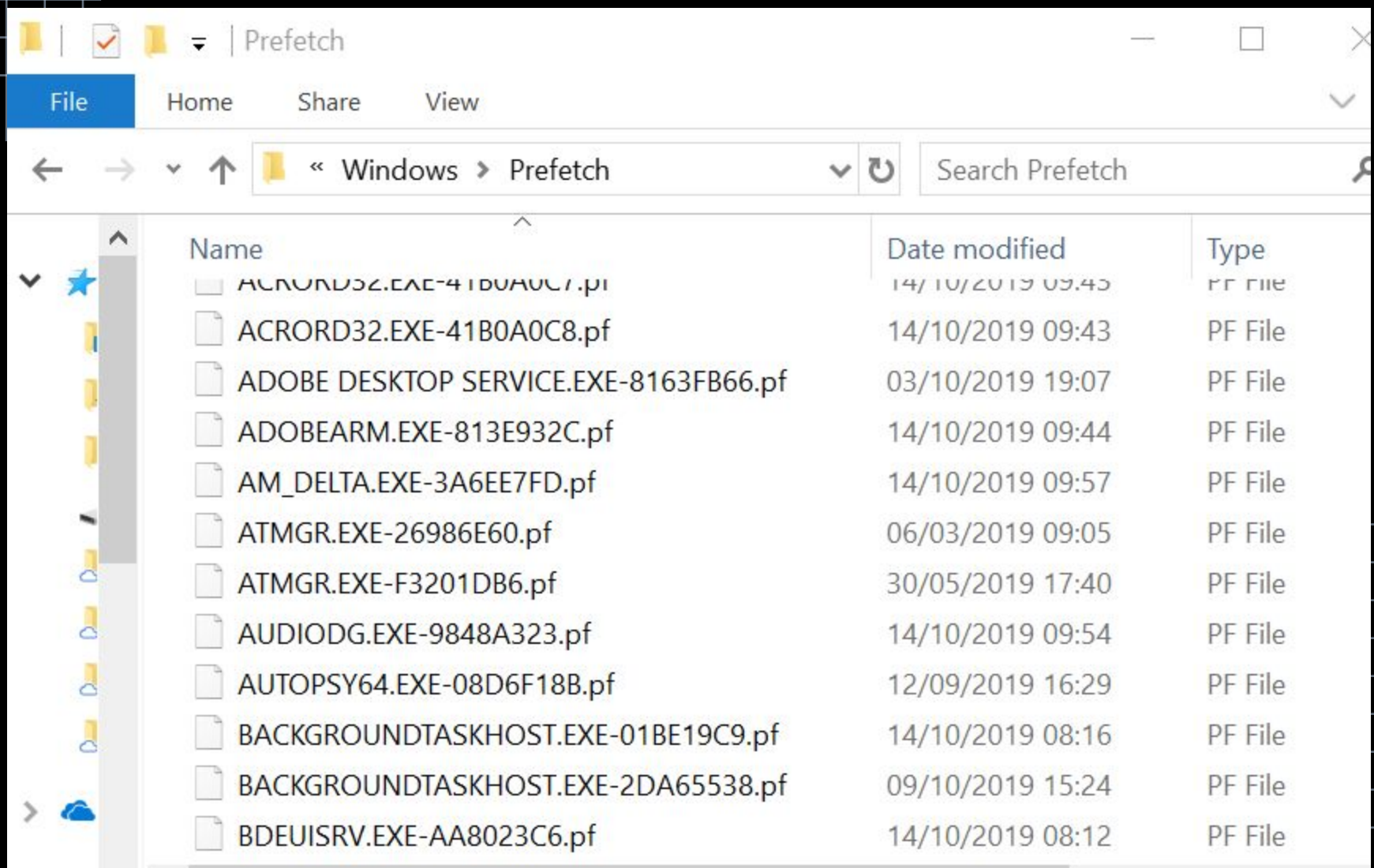
- Jump Lists are a windows feature introduced with Windows 7. They contain recently accessed applications and files.
- AUTOMATICALLY CREATED: Windows automatically creates jump lists for each application;
 - C:\Users\xxx\AppData\Local\Microsoft\Windows\Recent\AutomaticDestinations
- CUSTOMIZED: Users can customize jump lists by pinning or unpinning items; these are customized jump lists
 - C:\Users\xxx\AppData\Local\Microsoft\Windows\Recent\CustomDestinations



Spool Files

- Spool files – used by the system to store information about files sent to the printer
- C:\windows\System32\spool\PRINTERS
 - File's contents are written to a SPL file and a graphic (EMF) is produced for each page
 - Administrative information is also tracked via a shadow file (SHD) – contains information about user/machine name, document name and data type.
- Have to carve .SPL, .EMF and .SHD files as they are deleted after the printer completes the print job

Prefetch and Superfetch



Name	Date modified	Type
ACRORD32.EXE-41B0A0C7.pf	14/10/2019 09:43	PF File
ACRORD32.EXE-41B0A0C8.pf	14/10/2019 09:43	PF File
ADOBE DESKTOP SERVICE.EXE-8163FB66.pf	03/10/2019 19:07	PF File
ADOBEARM.EXE-813E932C.pf	14/10/2019 09:44	PF File
AM_DELTA.EXE-3A6EE7FD.pf	14/10/2019 09:57	PF File
ATMGR.EXE-26986E60.pf	06/03/2019 09:05	PF File
ATMGR.EXE-F3201DB6.pf	30/05/2019 17:40	PF File
AUDIODG.EXE-9848A323.pf	14/10/2019 09:54	PF File
AUTOPSY64.EXE-08D6F18B.pf	12/09/2019 16:29	PF File
BACKGROUNDTASKHOST.EXE-01BE19C9.pf	14/10/2019 08:16	PF File
BACKGROUNDTASKHOST.EXE-2DA65538.pf	09/10/2019 15:24	PF File
BDEUISRV.EXE-AA8023C6.pf	14/10/2019 08:12	PF File

Event Logs

The screenshot shows the Windows 'Computer Management' console. The left-hand tree view is expanded to 'Event Viewer' > 'Windows Logs' > 'Security'. The main pane displays a list of security events. The selected event, ID 4634, is shown in the details pane below. The details pane has two tabs: 'General' and 'Details'. The 'General' tab is active, showing a description of the event and a list of properties.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	16/10/2017 11:51:02	Microsoft ...	4735	Security Group
Audit Success	16/10/2017 11:51:02	Microsoft ...	4735	Security Group
Audit Success	16/10/2017 11:51:01	Microsoft ...	4634	Logoff
Audit Success	16/10/2017 11:51:01	Microsoft ...	4624	Logon
Audit Success	16/10/2017 11:51:01	Microsoft ...	4672	Special Logon
Audit Success	16/10/2017 11:29:21	Microsoft ...	4634	Logoff
Audit Success	16/10/2017 11:29:21	Microsoft ...	4634	Logoff
Audit Success	16/10/2017 11:29:21	Microsoft ...	4672	Special Logon

Event 4634, Microsoft Windows security auditing.

General Details

An account was logged off.

Subject:

Log Name: Security
Source: Microsoft Windows security auditing
Event ID: 4634
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online](#)

Logged: 16/10/2017 11:51:01
Task Category: Logoff
Keywords: Audit Success
Computer: S7L9829A63456B4.u

Actions

Security

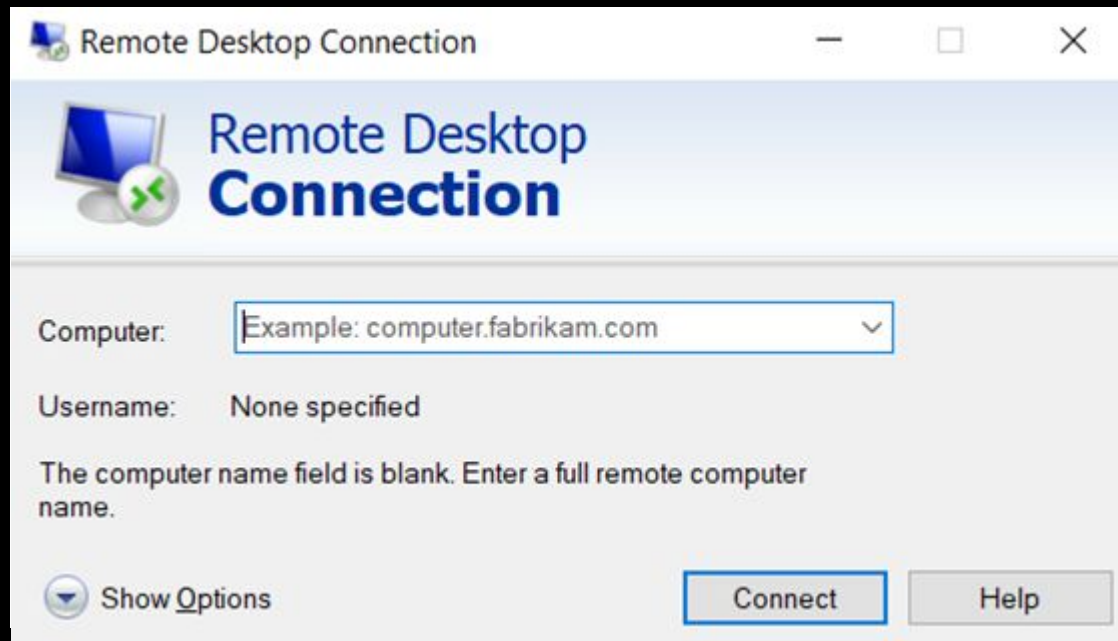
- Open Saved ...
- Create Custo...
- Import Custo...
- Clear Log...
- Filter Current ...
- Properties
- Find...
- Save All Even...
- Attach a Task...
- View
- Refresh
- Help
- Event 4634, Micro...
- Event Propert...
- Attach Task T...
- Copy
- Save Selecte...

Windows Error Reporting

- “The error reporting feature enables users to notify Microsoft of application faults, kernel faults, unresponsive applications, and other application specific problems” – Microsoft Docs
- C:\ProgramData\Microsoft\Windows\WER\ReportArchive
- C:\ProgramData\Microsoft\Windows\WER\ReportQueue
- C:\Users\XXX\AppData\Local\Microsoft\Windows\WER\ReportArchive
- C:\Users\XXX\AppData\Local\Microsoft\Windows\WER\ReportQueue

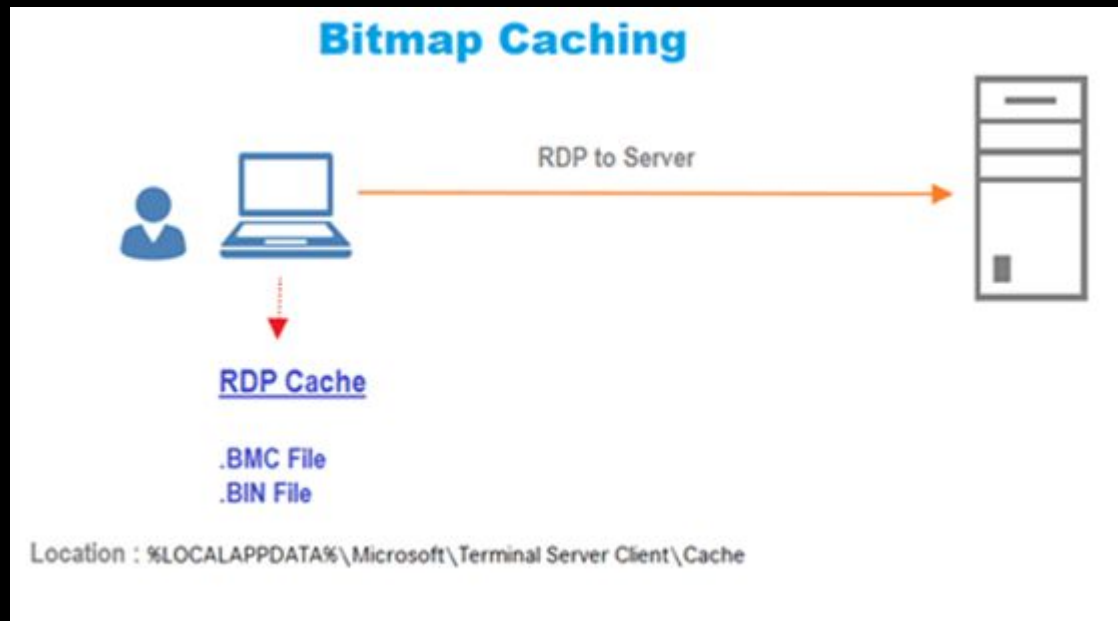
RDP Cache

- Remote Desktop Protocol (RDP) is a connection protocol developed by Microsoft to provide users with a graphical interface while connected to another computer over a network connection.



RDP Cache

- Remote Desktop Protocol (RDP) is a connection protocol developed by Microsoft to provide users with a graphical interface while connected to another computer over a network connection.

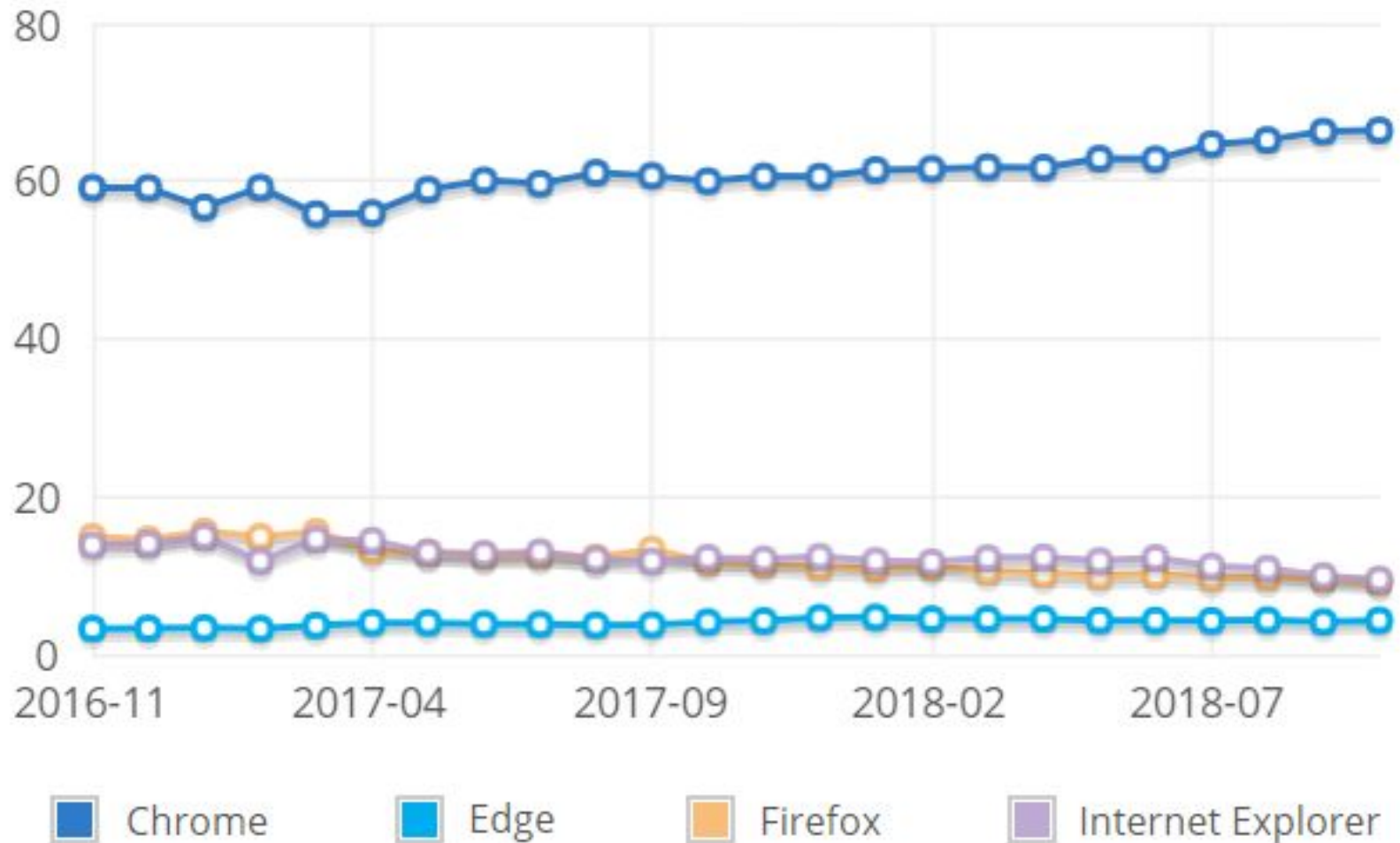


What is a browser?

- A HTTP client whose purpose is to :
 - Fetch documents from a remote server using the HTTP protocol
 - Render them in the window on the user's computer



Browser Market Share



Browser Artefacts

- History: is the list of web pages a user has visited, containing page title, time of visit...
- Cache: is a temporary storage location containing files downloaded by browsers to display websites, such as html files, CSS style sheets, JavaScript scripts...
- Cookies: are small pieces of information websites store on a person's computer, including a user ID, session ID, names, addresses...
- Searches: word/words that are typed into the browser "search" box

Browser Artefacts

Clear browsing data

Basic

Advanced

☒

Browsing history
19,209 items

☒

Download history
360 items

☒

Cookies and other site data
From 1,030 sites

☒

Cached images and files
294 MB

☒

Passwords and other sign-in data
None

☒

Auto-fill form data

Cancel

Clear data

Google Chrome

- Cache Location:

- C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default\Cache

- Cookies Location:

- C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default\Cookies

- History location:

- C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default\History

Mozilla Firefox

- Cache Location:

- C:\users\{username}\AppData\Local\Mozilla\Firefox\Profiles\xxxxx.default\cache2

- Cookies Location:

- C:\users\{username}\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxx.default\cookies.sqlite

- History location:

- C:\users\{username}\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxx.default\places.sqlite

Microsoft Edge

- Cache Location:

- C:\users\{username}\AppData\Local\Microsoft\Windows\WebCache

- Cookies Location:

- C:\users\{username}\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cookies

- History location:

- C:\users\{username}\AppData\Local\Microsoft\Windows\History

Conclusion

- Windows OSs are still the most popular platforms; therefore, it is critical that digital forensic investigators are familiar themselves with the technology.
- A deep understanding of how other OSs work will also help the investigation.