

System Configuration

- **Operating system version**
- **Control Set**
- **Computer name**
- **Timezone**
- **Network TCP/IP parameters**
- **Historical Network List**
- **Installed Applications**
- **Last shutdown**
- **Autoruns**

Operating System Version

SOFTWARE\Microsoft\Windows NT\CurrentVersion

Registry hives (3)				Available bookmarks (65/0)			
Enter text to search...				Find			
Key name	# values	# subkeys	Last write timestamp				
Windows Defender	11	14	2017-02-07 14:01:56				
Windows Desktop Search	1	0	2017-01-27 02:32:37				
Windows Embedded	0	1	2017-01-27 02:32:37				
Windows Mail	5	4	2016-07-16 11:48:34				
Windows Media Device Manager	1	3	2017-01-27 02:32:37				
Windows Media Foundation	0	8	2017-01-27 02:32:37				
Windows Media Player NSS	0	1	2017-01-27 02:32:37				
Windows Messaging Subsystem	1	1	2017-01-27 02:32:37				
Windows NT	0	1	2017-01-27 02:32:39				
CurrentVersion	27	87	2017-02-07 14:01:43				
Accessibility	0	2	2017-02-02 22:53:22				
AdaptiveDisplayBrightness	0	4	2017-01-27 02:32:39				
AeDebug	1	1	2017-01-27 02:32:39				
AppCompatFlags	3	17	2017-01-30 22:47:24				
ASR	1	0	2017-01-27 02:32:39				
Audit	0	1	2017-01-27 02:32:39				
BackgroundModel	2	11	2016-07-16 11:48:34				
ClipSVC	0	2	2016-07-16 11:48:34				
Compatibility32	1	0	2017-01-27 02:32:39				
Console	0	3	2017-01-27 02:32:42				
CorruptedFileRecovery	2	1	2017-01-27 02:32:39				
DefaultProductKey	3	0	2017-01-27 02:32:39				
DefaultProductKey2	3	0	2017-01-27 02:32:39				
DeviceDisplayObjects	1	6	2016-07-16 11:48:34				
DiskDiagnostics	0	2	2017-01-27 02:32:39				
drivers.desc	3	0	2017-01-27 02:36:31				
Drivers32	24	0	2017-01-27 02:37:50				
EFS	0	2	2017-01-27 02:32:39				
EMDMgmt	0	7	2017-02-07 14:02:42				
Event Viewer	3	0	2017-01-27 02:32:39				

Values			
Drag a column header here to group by that column			
Value Name	Value Type	Data	Value Slack
SystemRoot	RegSz	C:\WINDOWS	00-00-00-00-00-00
BuildBranch	RegSz	rs1_release	20-00-00-00
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffff	CB-19
BuildLab	RegSz	14393.rs1_release.161220-1747	
BuildLabEx	RegSz	14393.693.amd64fre.rs1_release.161220-1747	00-00-00-00-00-00
CompositionEditionID	RegSz	Professional	00-00
CurrentBuild	RegSz	14393	
CurrentBuildNumber	RegSz	14393	
CurrentMajorVersionNumber	RegDword	10	
CurrentMinorVersionNumber	RegDword	0	
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00-00
CurrentVersion	RegSz	6.3	68-F9-FD-01
EditionID	RegSz	Professional	00-00
InstallationType	RegSz	Client	00-00-00-00-00-00
InstallDate	RegDword	1485485927	
ProductName	RegSz	Windows 10 Pro	74-00-65-00-72-00-00-00-00-00-00-00-00
ReleaseId	RegSz	1607	FD-01
SoftwareType	RegSz	System	FD-01-D8-FC-FD-01
UBR	RegDword	693	
PathName	RegSz	C:\WINDOWS	37-03-F0-C1-37-03
Customizations	RegSz	ModernApps	7F-03-80-E7-7F-03
ProductId	RegSz	00330-50295-68670-AAOEM	00-00-00-00
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-33-30-2D-35...	
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-35-00-35-00-30-00-34...	00-00-00-00
RegisteredOrganization	RegSz	Hewlett-Packard Company	61-67-65-5F
RegisteredOwner	RegSz	Sarah McAvoy	00-00
InstallTime	RegQword	131299595279901393	00-00-00-00

Operating System SOFTWARE

/version

Values

Data Interpreter

Numbers

8 bit, signed	-47
8 bit, unsigned	209
16 bit, signed	-23,855
16 bit, unsigned	41,681
32 bit, signed	1,204,789,969
32 bit, unsigned	1,204,789,969
64 bit, signed	131,299,595,279,901,393
64 bit, unsigned	131,299,595,279,901,393
Float	106309.6
Double	6.89490240134473E-300

Dates and times

DOS FAT Time/date (32 bit)	n/a
DOS FAT Date/time (32 bit)	n/a
Unix/Posix (32 bit)	2008-03-06 07:52:49
Windows FILETIME (64 bit)	2017-01-27 02:58:47
OLE 2.0 Date/time (64 bit)	1899-12-30 00:00:00
Windows SYSTEM Date/time (128 bit)	n/a

Other

GUID	n/a
Maps to	n/a
IP Address	209.162.207.71
Product Key (<= Win7)	n/a
Product Key (>= Win8)	n/a

Strings

ASCII	ÑđİGİxÖ□
Unicode	ð鏢磗
To Base64	0aLPR0l40gE=
From Base64	n/a

NOTE: Data is interpreted from the current offset and is not based on the selected bytes

Offset: 0 (0x0) Always on top ?

InstallTime RegQword 131299595279901393 00-00-00-00

Current Control Set

SYSTEM\Select

Registry hives (3) Available bookmarks (65/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
D:\UNIGE\HD1\SYSTEM_clean	=	=	=
ROOT	0	15	2017-02-07 14:01:22
ActivationBroker	0	1	2017-01-27 02:32:39
ControlSet001	0	6	2017-01-27 02:32:40
DriverDatabase	3	4	2017-01-27 02:53:14
HardwareConfig	2	1	2017-02-07 14:01:22
Input	0	1	2017-01-27 02:32:39
Keyboard Layout	0	2	2017-01-27 02:32:39
Maps	1	1	2017-01-27 02:53:32
MountedDevices	6	0	2017-02-07 14:01:35
ResourceManager	2	4	2017-01-27 02:32:39
ResourcePolicyStore	0	2	2017-01-27 02:32:39
RNG	2	0	2017-02-07 14:01:22
Select	4	0	2017-01-27 02:32:39
Setup	20	13	2017-02-07 14:02:15
Software	0	1	2017-01-27 02:32:40
WPA	0	7	2017-02-06 19:19:44
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	799	0	
D:\UNIGE\HD1\SOFTWARE_clean			
E:\Windows\System32\config\SAM			2017-01-27 05:27:19

Values

Drag a column header here to group by that column

Value Name	Value Type	Data
Current	RegDword	1
Default	RegDword	1
Failed	RegDword	0
LastKnownGood	RegDword	1

Computer Name

SYSTEM\Current Control Set\Control\ComputerName\ComputerName

The screenshot displays the Windows Registry Editor. The left pane shows the tree structure expanded to **SYSTEM\Current Control Set\Control\ComputerName\ComputerName**. The right pane shows the values for this path. The 'ComputerName' value is highlighted with a red box.

Key name	# values	# subkeys	Last write timestamp
D:\UNIGE\HD1\SYSTEM_clean	=	=	=
ROOT	0	15	2017-02-07 14:01:22
ActivationBroker	0	1	2017-01-27 02:32:39
ControlSet001	0	6	2017-01-27 02:32:40
Control	11	112	2017-02-07 14:01:50
ACPI	1	0	2017-01-27 02:32:40
AppID	0	2	2017-01-27 02:32:40
AppReadiness	1	0	2016-07-16 11:48:30
Arbiters	0	3	2017-01-27 02:32:40
BackupRestore	0	3	2017-01-27 02:32:40
BitLocker	1	0	2017-01-27 02:45:44
CI	0	3	2017-01-27 02:45:41
Class	0	106	2017-01-27 17:46:08
CMF	2	4	2017-01-27 02:58:09
CoDeviceInstallers	0	0	2017-01-27 02:32:40
COM Name Arbiter	0	0	2017-01-27 02:32:40
CommonGlobUserSettings	0	1	2017-01-27 02:32:40
Compatibility	0	1	2017-01-27 02:32:40
ComputerName	0	1	2017-02-07 14:01:41
ComputerName	2	0	2017-01-27 02:32:40

Value Name	Value Type	Data
(default)	RegSz	mnmsrvc
ComputerName	RegSz	DESKTOP-KLOQJ0V

Timezone

SYSTEM\Current Control Set\Control\TimeZoneInformation

Registry hives (3)				Available bookmarks (65/0)			Values		
Enter text to search...				Find			TimeZoneInformation		
Key name	# values	# subkeys	Last write timestamp				Value Name	Value Data	Value Data Raw
Terminal Server	16	12	2017-02-07 14:01:43				Bias	300	300
TimeZoneInformation	10	0	2017-01-27 02:32:40				DaylightBias	-60	4294967236
Ubpm	21	0	2016-07-16 11:48:29				DaylightName	@tzres.dll,-111	@tzres.dll,-111
usb	1	1	2017-01-27 02:32:40				DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00-00
usbflags	0	9	2017-02-06 19:42:05				StandardBias	0	0
usbstor	0	5	2017-01-27 02:32:40				StandardName	@tzres.dll,-112	@tzres.dll,-112
VAN	0	5	2016-07-16 11:48:29				StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-08-00-01-00-02-00-00-00-00-00-00-00-00-00-00
Video	0	2	2017-01-27 02:35:28				TimeZoneKeyName	Eastern Standard Time	Eastern Standard Time
WalletService	1	0	2016-07-16 11:48:29				ActiveTimeBias	300	300
wcnscvc	0	2	2017-01-27 02:32:40						
Wdf	0	4	2017-01-27 02:32:40						
WDI	0	3	2016-07-16 11:48:29						
Windows	12	0	2017-01-30 22:46:43						
WinInit	1	0	2017-01-27 02:32:40						
Winlogon	0	1	2017-01-27 02:32:40						
WMI	0	3	2017-01-27 02:32:40						

Services

SYSTEM\CurrentControlSet\Services

Registry hives (3)				Available bookmarks (65/0)						
Enter text to search...				Find						
Key name	# values	# subkeys	Last write timestamp							
Hardware Profiles	0	3	2017-02-07 14:01:22							
Policies	0	0	2017-01-27 02:32:40							
Services	0	656	2017-02-02 22:53:22							
.NET CLR Data	0	2	2017-01-27 02:32:40							
.NET CLR Networking	0	2	2017-01-27 02:32:40							
.NET CLR Networking 4.0.0.0	0	2	2017-01-27 02:32:40							
.NET Data Provider for Oracle	0	2	2017-01-27 02:32:40							
.NET Data Provider for SqlServer	0	2	2017-01-27 02:32:40							
.NET Memory Cache 4.0	0	2	2017-01-27 02:32:40							
.NETFramework	0	1	2017-01-27 02:32:40							
1394ohci	6	0	2017-01-27 02:32:40							
3ware	7	2	2017-01-27 02:32:40							
Accelerometer	8	3	2017-02-07 14:01:22							
ACPI	8	1	2017-02-07 14:01:22							
AcpiDev	8	0	2017-01-27 02:32:40							
acpiex	7	1	2017-01-27 02:32:40							
acpipagr	6	1	2017-02-07 14:01:22							
AcpiPmi	6	0	2017-01-27 02:32:40							
acptime	8	0	2017-01-27 02:32:40							
ADOVMPPackage	0	1	2017-01-27 02:32:40							
ADP80XX	7	2	2017-01-27 02:32:40							
adsi	0	3	2017-01-27 02:32:40							
AFD	8	1	2017-01-27 02:32:40							
agp440	0	1	2017-01-27 02:32:40							
ahcache	6	0	2017-01-27 02:32:40							
AJRouter	9	3	2017-01-27 02:32:40							
ALG	10	0	2017-01-27 02:32:40							
AmdK8	8	0	2017-01-27 02:32:40							
AmdPPM	8	0	2017-01-27 02:32:40							
amdsata	7	2	2017-01-27 02:32:40							
amdsbs	7	3	2017-01-27 02:32:40							

Values Services										
Drag a column header here to group by that column										
Name	Description	Display Name	Start Mode	Service Type	Name Key Last Write	Parameters Key Last...	Group	Image Path	Service DLL	
TabletInputService	@%SystemRoot%\system32\TabSvc.dll,-101	@%SystemRoot%\system32\TabSvc.dll,-100	Manual	Win32ShareProcess	2017-01-27 02:32:40	2017-01-27 02:32:40	PlugPlay	%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted	%SystemRoot%\System32\TabSvc.dll	
TapiSrv	@%SystemRoot%\system32\tapisrv.dll,-101	@%SystemRoot%\system32\tapisrv.dll,-100	Manual	Win32ShareProcess	2017-01-27 02:32:40	2017-01-27 02:32:40		%SystemRoot%\System32\svchost.exe -k NetworkService	%SystemRoot%\System32\tapisrv.dll	
Tcpip	@%SystemRoot%\system32\tcpipcfg.dll,-50003	@%SystemRoot%\system32\tcpipcfg.dll,-50003	Boot	KernelDriver	2017-01-27 02:32:40	2017-02-02 21:24:28	PNP_TDI	System32\drivers\tcpip.sys		
Tcpip6	@todo.dll,-100;Microsoft IPv6 Protocol Driver	@todo.dll,-100;Microsoft IPv6 Protocol Driver	Manual	KernelDriver	2017-01-27 02:32:40	2017-01-27 02:45:39		System32\drivers\tcpip.sys		
TCPIP_TUNNEL			Disabled	Adapter	2017-01-27 02:32:40					
tcpipreg	Provides compatibility for legacy applications which interact with TCP/IP through the registry. If this service is stopped, certain applications may have impaired functionality.	TCP/IP Registry Compatibility	Automatic	KernelDriver	2017-01-27 02:32:40			System32\drivers\tcpipreg.sys		
TDI			Disabled	Adapter	2017-01-27 02:32:40					
tdx	@%SystemRoot%\system32\tcpipcfg.dll,-50004	@%SystemRoot%\system32\tcpipcfg.dll,-50004	System	KernelDriver	2017-01-27 02:32:40		PNP_TDI	SystemRoot\system32\DRIVERS\tdx.sys		
termintp		@termmou.inf,%TermIntp.SVCDESC%:Micro	Manual	KernelDriver	2017-01-27 02:32:40		Extended Base	SystemRoot\System32\drivers\termintp.sys		

Network TCP/IP Parameters

SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

Registry Explorer v1.5.2.0

File Tools Options Bookmarks (27/0) View Help

Registry hives (1) Available bookmarks (27/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
ControlSet001\services\Tcpip\Parameters\Interfaces	=	=	=
swprv	10	1	2019-03-19 04:53:37
Synth3dVsc	7	0	2019-03-19 04:52:29
Synth3dVsp	5	0	2020-04-17 22:32:56
SynTP	7	1	2020-04-17 22:32:56
SynTPEnhService	8	1	2020-01-08 12:26:34
SysMain	14	1	2019-03-19 04:53:37
SystemEventsBroker	11	3	2019-03-19 04:54:23
TabletInputService	12	3	2019-03-19 04:54:23
TapiSrv	11	3	2019-03-19 04:53:37
Tcpip	13	5	2020-01-08 20:49:36
Linkage	3	0	2020-04-17 22:33:41
Parameters	12	6	2020-04-20 17:05:38
Adapters	0	15	2020-04-17 22:33:41
DNSRegisteredAdapters	0	0	2020-01-08 20:49:51
Interfaces	0	16	2020-04-17 22:33:41
{0f42d155-a0c4-4e82-9a8e-0898bccf8df3}	22	4	2020-04-20 17:05:38
27E6379737	21	0	2020-03-01 19:38:40
8686F6E6F62737	23	0	2020-02-06 19:26:18
940586F6E65685	21	0	2020-04-18 09:16:40
960586F6E656	21	0	2020-01-17 14:23:11
{12af19fe-959b-4fd8-8b4...	3	0	2020-04-08 07:50:45
{32b46da3-776a-494b-88c...	3	0	2020-01-08 20:53:20
{3820e9cc-fd73-4ef3-a20...	14	0	2020-04-03 17:22:27
{4181adcd-f6f6-4922-84c...	3	0	2020-01-08 20:49:53

Key: ControlSet001\services\Tcpip\Parameters\Interfaces

Value: None Collapse all hives

Selected hive: SYSTEM Last write: 2020-04-17 22:33:41 Key contains no values Load complete Hidden keys: 0 7

Values DHCPNetworkHints

Drag a column header here to group by that column

Network Hint	DHCP Address	DHCP Server	DHCP Domain	Lease Obtained	Lease Expires	Default Gateway	Interface	Interface Subkey
Vodafone-30452471	192.168.1.6	192.168.1.1	station	2020-04-20 17:05:38	2020-04-20 18:05:38	192.168.1.1	{0f42d155-a0c4-4e82-9a8e-0898bccf8df3}	{0f42d155-a0c4-4e82-9a8e-0898bccf8df3}
rnsys	10.9.9.20	10.9.9.1		2020-02-28 18:22:47	2020-03-06 18:22:47	10.9.9.1	{0f42d155-a0c4-4e82-9a8e-0898bccf8df3}	27E6379737
hhonors	10.20.6.153	10.20.0.11	controllers	2020-02-06 15:08:26	2020-02-06 23:08:26	10.20.0.11	{0f42d155-a0c4-4e82-9a8e-0898bccf8df3}	8686F6E6F62737
IPhoneX	172.20.10.5	172.20.10.1		2020-04-17 19:43:49	2020-04-18 19:29:25	172.20.10.1	{0f42d155-a0c4-4e82-9a8e-0898bccf8df3}	940586F6E65685
iPhone	172.20.10.2	172.20.10.1		2020-01-17 10:09:38	2020-01-18 09:55:14	172.20.10.1	{0f42d155-a0c4-4e82-9a8e-0898bccf8df3}	960586F6E656

Total rows: 5 Export ?

Type viewer

Network List

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList

Registry Explorer v1.5.2.0

File Tools Options Bookmarks (18/0) View Help

Registry hives (2) Available bookmarks (45/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Devices	0	46	2020-04-19 15:56:55
Image File Execution Options	0	56	2020-04-18 18:38:16
Internet Explorer	9	33	2020-04-17 22:32:25
LogonUI	9	13	2020-04-20 08:04:59
NetworkCards	0	6	2020-04-10 20:35:30
NetworkList	3	6	2020-01-08 21:02:38
Products	0	55	2020-04-20 10:01:45
Products	0	55	2020-04-20 10:01:45
Run	5	0	2020-04-20 10:01:45
StartMenuInternet	1	2	2020-01-08 12:41:23
System	21	2	2020-01-08 20:49:47

Bookmark information

Hive: C:\Windows\system32\config\SOFTWARE

Category: Network

Name: NetworkList

Key path: Microsoft\Windows NT\CurrentVersion\NetworkList

Short description: Contains information about networks a computer has connected to

Long description: A plugin exists for this key

Key: Microsoft\Windows NT\CurrentVersion\NetworkList

Selected hive: SOFTWARE Last write: 08/01/2020 21:02:38 +00:00 3 of 3 values shown (100,00%)

Values Known networks

Drag a column header here to group by that column

Network Name	Name Type	First Connect LOCAL	Last Connected LOCAL	Managed	DNS Suffix	Gateway Mac Addr ...	Profile GUID
rnsys	Wireless	2020-01-08 13:02:38	2020-02-28 19:22:47	<input type="checkbox"/>	<none>	00-09-0F-09-00-01	{C910B85E-221F-4405-A4F3-11E822C7564B}
The Sans	Wireless	2020-03-01 20:38:40	2020-03-07 08:48:24	<input type="checkbox"/>	<none>	00-50-E8-04-53-73	{8ACF9933-EC16-409A-BFAD-46551AD7E0C7}
GenuaWifi	Wireless	2020-01-17 09:57:14	2020-01-18 09:07:24	<input type="checkbox"/>	wifi.unige.local	04-09-73-67-E1-00	{7B711108-1971-4118-9BBC-4219465E2F3B}
hhonors	Wireless	2020-02-02 23:04:53	2020-02-06 16:08:27	<input type="checkbox"/>	controllers	08-35-71-03-CE-B2	{78AC8A7D-1A19-48C9-A272-0D2266615944}
Network	Wireless	2020-03-04 11:20:54	2020-04-17 21:43:49	<input type="checkbox"/>	<none>	46-18-FD-E9-BC-64	{374E77B2-0768-4B47-A4C5-24FD55ECBEAB}
Vodafone-30452471	Wireless	2020-01-16 23:13:03	2020-04-20 10:05:39	<input type="checkbox"/>	station	90-35-6E-CB-69-60	{E5AE389F-1A69-461D-9538-553DF2CC3ACC}
FOR585	Wireless	2020-02-03 15:17:37	2020-02-07 20:22:26	<input type="checkbox"/>	<none>	B8-69-F4-58-58-39	{9847A354-5716-4C67-A1C1-54E565F82700}
iPhone	Wireless	2020-01-17 09:59:13	2020-01-17 09:59:13	<input type="checkbox"/>	<none>	FA-95-EA-E1-50-64	{297EA78E-9B71-438D-87AC-4CAF9ED7D521}

Total rows: 8

Type viewer Slack viewer

Value name (default)

Value: (default) Collapse all hives

Hidden keys: 0 13

Installed Applications

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Registry hives (3)				Available bookmarks (65/0)			
Enter text to search...				Find			
Key name	# values	# subkeys	Last write timestamp				
{93CB4DD0-E7C1-4800-9B55-8F99...}	24	0	2017-01-27 02:47:44				
{98A452E7-A559-4687-A58C-0C6A...}	24	0	2017-01-27 02:47:44				
{A749D8E6-B613-3BE3-8F5F-045C...}	25	0	2017-01-27 02:47:44				
{ad8a2fa1-06e7-4b0d-927d-6e54b...}	25	0	2017-01-27 02:47:44				
{C1B938F9-9874-4920-8FED-D5CA...}	24	0	2017-01-27 02:47:44				
{CF2BEA3C-26EA-32F8-AA9B-331F...}	25	0	2017-01-27 02:47:44				
{D1E8F2D7-7794-4245-B286-...}	25	0	2017-01-27 02:47:44				
{DC5AEDF6-DCDB-499A-8A72-AB6...}	24	0	2017-01-27 02:47:44				
{E0E5975B-6D35-48FF-98F9-3064...}	25	0	2017-01-27 02:47:44				
URL	0	2	2017-01-27 02:32:38				
UserPictureChange	1	0	2016-07-16 11:48:34				
UserState	0	1	2017-01-27 02:32:38				
WebCheck	2	0	2017-01-27 02:32:38				
WinBio	0	2	2017-01-27 02:32:38				
Windows Block Level Backup	2	0	2017-01-27 02:32:38				
Windows To Go	1	0	2017-01-27 02:32:38				
WindowsAnytimeUpgrade	0	0	2016-07-16 11:49:10				
WindowsBackup	0	0	2017-01-27 02:32:38				
WindowsStore	0	1	2017-01-27 02:32:38				
WindowsUpdate	3	5	2017-02-02 22:50:45				
WINEVT	0	3	2017-01-27 02:32:38				
Wordpad	0	1	2017-01-27 02:32:38				
WSMAN	2	8	2017-01-27 02:55:57				
XWizards	0	3	2017-01-27 02:32:39				
DWM	7	0	2017-02-07 14:01:43				
EnterpriseResourceManager	0	1	2017-01-27 02:32:37				
HTML Help	2	0	2017-01-27 02:32:37				
ITStorage	0	1	2016-07-16 11:48:34				

Values			
Drag a column header here to group by that column			
Value Name	Value Type	Data	Value Slack
AuthorizedCDFPrefix	RegSz		
Comments	RegSz		
Contact	RegSz		
DisplayVersion	RegSz	1.2.8334.5401	
HelpLink	RegSz		
HelpTelephone	RegSz		
InstallDate	RegSz	20170126	71-04
InstallLocation	RegSz	c:\Program Files (x86)\Hewlett-Packard\HP Regis...	00-00-00-00
InstallSource	RegSz	c:\SWSETUP\APP\PreReq2\HP\HPSetupIn_LLM...	00-00-00-00
ModifyPath	RegExpandSz	MsiExec.exe /X{D1E8F2D7-7794-4245-B286-87E...}	00-00
NoModify	RegDword	1	
NoRepair	RegDword	1	
Publisher	RegSz	Hewlett-Packard	00-00-00-00
Readme	RegSz		
Size	RegSz		
EstimatedSize	RegDword	34018	
UninstallString	RegExpandSz	MsiExec.exe /X{D1E8F2D7-7794-4245-B286-87E...}	00-00
URLInfoAbout	RegSz	http://www.Hewlett-Packard.com	00-00-00-00-00-00
URLUpdateInfo	RegSz		
VersionMajor	RegDword	1	
VersionMinor	RegDword	2	
WindowsInstaller	RegDword	1	
Version	RegDword	16916622	
Language	RegDword	1033	
DisplayName	RegSz	HP Registration Service	F0-2D-71-04

Installed Applications

SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Registry Editor window showing the path **SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall**. The left pane displays a list of installed applications, with **Google Chrome** selected. The right pane displays the registry values for Google Chrome.

Value Name	Value Type	Data	Value Slack	Is
DisplayName	RegSz	Google Chrome		
UninstallString	RegSz	"C:\Program Files (x86)\Google\Chro...	00-00	
InstallLocation	RegSz	C:\Program Files (x86)\Google\Chrom...	8A-04	
DisplayIcon	RegSz	C:\Program Files (x86)\Google\Chrom...		
NoModify	RegDword	1		
NoRepair	RegDword	1		
Publisher	RegSz	Google Inc.	00-00-00-00	
Version	RegSz	56.0.2924.87	2B-02	
DisplayVersion	RegSz	56.0.2924.87	2B-02	
InstallDate	RegSz	20170126	89-04	
VersionMajor	RegDword	2924		
VersionMinor	RegDword	87		

Shutdown Time

SYSTEM\Current Control Set\Control\Windows

The screenshot displays the Windows Registry Editor with the path `SYSTEM\Current Control Set\Control\Windows` selected. The left pane shows the tree structure, and the right pane shows the values. The `ShutdownTime` value is highlighted in red. The Data Interpreter pane on the right shows the interpretation of the selected value, which is `Windows FILETIME (64 bit)` with the value `2017-01-30 22:46:43`.

Value Name	Value Type	Data
ComponentizedBuild	RegDword	1
CSDBuildNumber	RegDword	0
CSDReleaseType	RegDword	0
CSDVersion	RegDword	0
Directory	RegExpandSz	%SystemRoot%
ErrorMode	RegDword	0
FullProcessInformationSID	RegBinary	01-06-00-00-00-00-05-50-00
NoInteractiveServices	RegDword	1
ShellErrorMode	RegDword	1
SystemDirectory	RegExpandSz	%SystemRoot%\system32
ShutdownTime	RegBinary	DD-4C-9B-BA-4A-7B-D2-01
ShutdownStopTimePerfCounter	RegQword	710011434274

Numbers	
8 bit, signed	-35
8 bit, unsigned	221
16 bit, signed	19,677
16 bit, unsigned	19,677
32 bit, signed	-1,164,227,363
32 bit, unsigned	3,130,739,933
64 bit, signed	131,302,900,035,701,981
64 bit, unsigned	131,302,900,035,701,981
Float	-0.001184847
Double	6.89928532503162E-300

Dates and times	
DOS FAT Time/date (32 bit)	2073-04-27 09:38:58
DOS FAT Date/time (32 bit)	2018-06-29 23:20:54
Unix/Posix (32 bit)	1933-02-09 03:30:37
Windows FILETIME (64 bit)	2017-01-30 22:46:43
OLE 32-bit Date/time (64 bit)	1633-12-30 00:00:00
Windows SYSTEM Date/time (128 bit)	n/a

Other	
GUID	n/a
Maps to	n/a
IP Address	221.76.155.186
Product Key (<= Win7)	n/a
Product Key (>= Win8)	n/a

Strings	
ASCII	ŸŁ,oj{Ö□
Unicode	鸚鵡發δ
To Base64	3Uybukp70gE=
From Base64	n/a

NOTE: Data is interpreted from the current offset and is not based on the selected bytes

Offset: 0 (0x0) Always on top ?

Autorun

SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Registry Explorer v1.5.2.0

File Tools Options Bookmarks (20/0) View Help

Registry hives (1) Available bookmarks (20/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Devices	0	0	2009-07-14 04:49:00
EMDMgmt	0	5	2015-03-24 21:02:34
Image File Execution Options	0	10	2015-03-22 15:19:29
Internet Explorer	9	33	2015-03-22 15:19:29
LastConnect	1	0	2015-03-25 10:15:21
LogonUI	4	2	2015-03-25 13:05:47
NetworkCards	0	1	2015-03-25 10:17:16
8	2	0	2015-03-25 10:17:16
NetworkList	2	5	2015-03-22 15:08:24
Products	0	32	2015-03-25 15:19:05
Products	0	32	2015-03-25 15:19:11
Run	1	0	2015-03-25 14:57:31
StartMenuInternet	1	2	2015-03-22 15:11:52
System	16	1	2009-07-14 05:01:33
System	16	1	2009-07-14 05:01:33
Windows Portable Devices	0	2	2009-07-14 04:49:00
Winlogon	21	1	2015-03-25 13:05:43

Bookmark information

Hive: D:\UNIGE_2020\Data_Leakage_Extracted\SOFTWARE

Category: Autoruns

Name: Run

Key path: Microsoft\Windows\CurrentVersion\Run

Short description: Run key

Long description: Used to automatically start programs

Key: Microsoft\Windows\CurrentVersion\Run

Selected hive: SOFTWARE Last write: 25/03/2015 14:57:31 +00:00 1 of 1 values shown (100,00%)

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	I...	Data Record Reallocated
Eraser	RegSz	"C:\Program Files\Eraser\Eraser.exe" /atRestart		

Type viewer Slack viewer Binary viewer

Value name: Eraser

Value type: RegSz

Value: "C:\Program Files\Eraser\Eraser.exe" /atRestart

Raw value: 22-00-43-00-3A-00-5C-00-50-00-72-00-6F-00-67-00-72-00-61-00-6D-00-20-00-46-00-69-00-6C-00-65-00-73-00-5C-00-45-00-72-00-61-00-73-00-65-00-72-00-2E-00-65-00-78-00-65-00-22-00-20-00-2F-00-61-00-74-00-52-00-65-00-73-00-74-00-61-00-72-00-74-00-00-00

UniGe 2025 – DFIR – Windows

Value: Eraser Collapse all hives

Hidden keys: 0 1

Exercise 4

1. Which **TCP/IP information** can you find in the registry?

- IP Address
- Subnet Mask
- Name Server
- Domain
- Default Gateway
- Network type
- Connection timestamps

2. When was **Google Chrome** installed?

3. When was **Skype** installed?

Exercise 4.1

Registry hives (3)

Available bookmarks (65/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
Parameters	13	6	2017-02-02 21:24:28
Adapters	0	11	2017-01-27 02:37:53
DNSRegisteredAdapters	0	0	2017-01-27 02:32:54
Interfaces	0	12	2017-01-27 02:37:53
NsiObjectSecurity	0	0	2016-07-16 11:48:29
PersistentRoutes	0	0	2016-07-16 11:48:29
Winsock	7	3	2016-07-16 11:49:24
Performance	5	0	2017-01-27 02:32:40

Values

DHCPNetworkHints

NetworkSettings

Drag a column header here to group by that column

Network Hint	DHCP Address	DHCP Server	DHCP Domain	Lease Obtained	Lease Expires	Default Gateway	Interface	Interface Subkey
MU WIFI	10.104.236.66	10.101.4.43	wireless.marshall.edu	2017-02-02 22:39:28	2017-02-02 23:09:28	10.104.236.2	{e27334ec-22dc-48fc-b57b-06fb46bb7c47}	{e27334ec-22dc-48fc-b57b-06fb46bb7c47}
MU_Guest	10.102.200.253	10.101.4.43	guest.marshall.edu	2017-01-30 22:45:44	2017-01-30 23:45:44	10.102.200.2	{e27334ec-22dc-48fc-b57b-06fb46bb7c47}	D455F57457563747

Registry hives (3)				Available bookmarks (65/0)					
Enter text to search...				Find					
Key name	# values	# subkeys	Last write timestamp						
IniFileMapping	0	5	2017-01-27 02:32:39						
KnownFunctionTableDlls	2	0	2017-01-27 02:32:39						
KnownManagedDebuggingDlls	3	0	2017-01-27 02:32:39						
LanguagePack	1	2	2017-01-27 02:32:42						
LicensingDiag	1	0	2017-01-27 02:32:39						
MCI Extensions	50	0	2017-01-27 02:32:39						
MCI32	5	0	2017-01-27 02:32:39						
MiniDumpAuxiliaryDlls	5	0	2017-01-27 02:32:39						
MsiCorruptedFileRecovery	0	1	2017-01-27 02:32:39						
Multimedia	0	1	2017-01-27 02:32:39						
NetworkCards	0	2	2017-01-27 02:37:51						
NetworkList	3	6	2017-01-27 02:45:44						
DefaultMediaCost	5	0	2016-07-16 11:48:34						
NewNetworks	1	0	2017-01-28 21:41:14						
Nla	0	2	2017-01-27 02:45:44						

Values									
Known networks									
Drag a column header here to group by that column									
First Network	Network Name	Name Type	First Connect LOCAL	Last Connected LOCAL	Managed	DNS Suffix	Gateway Mac Address	Profile GUID	
McDonalds Free WIFI	McDonalds Free WIFI	Wireless	2017-01-28 16:41:14	2017-01-28 16:41:14	<input checked="" type="checkbox"/>	mcd01461.pit.wayport.net	00-90-FB-36-0E-50	{53993B86-C125-40F2-84A0-FD2355EE4898}	
MU_Guest	MU_Guest	Wireless	2017-01-26 21:20:55	2017-01-30 17:45:44	<input type="checkbox"/>	guest.marshall.edu	00-00-0C-07-AC-01	{8F152B6E-7584-479C-88D1-84DAC75ADD03}	
MU_WIFI	MU_WIFI	Wireless	2017-01-26 18:24:16	2017-02-02 16:24:28	<input type="checkbox"/>	resnet.marshall.edu	00-00-0C-07-AC-01	{DA597274-234F-4C43-9500-FBB518E2F8C9}	

Exercise 4.2/4.3

Registry hives (3)				Available bookmarks (65/0)									
Enter text to search...				Find									
Key name	# values	# subkeys	Last write timestamp										
≡	=	=	=										
PushNotifications	0	1	2017-01-27 02:32:42										
Reliability	1	2	2017-01-27 02:32:42										
Run	7	0	2017-01-27 02:47:49										
RunOnce	0	0	2017-01-27 02:32:42										
Security and Maintenance	0	1	2017-01-27 02:32:42										
SettingSync	5	7	2017-01-27 02:32:42										
SharedDlls	402	0	2017-01-30 18:47:47										
Shell Extensions	0	2	2017-01-27 02:32:42										
ShellCompatibility	0	5	2017-01-27 02:32:42										
ShellServiceObjectDelayLoad	1	0	2017-01-27 02:32:42										
SmartGlass	0	0	2017-01-27 02:32:42										
SMDEn	0	0	2017-01-27 02:32:42										
Store	0	2	2017-01-27 02:32:42										
Synmgr	1	2	2017-01-27 02:32:42										
SysPrepTapi	0	0	2017-01-27 02:32:42										
Telephony	0	3	2017-02-07 14:01:40										
Themes	5	3	2017-01-27 02:32:42										
TouchKeyboard	0	1	2017-01-27 02:32:42										
Uninstall	0	76	2017-01-27 02:47:49										
AddressBook	0	0	2017-01-27 02:32:42										
Connection Manager	1	0	2017-01-27 02:32:42										

Values Uninstall									
Drag a column header here to group by that column									
Timestamp	Key Name	Display Name	Display Version	Publisher	Install Date	Install Source	Install Location	Uninstall String	
≡	≡	≡	≡	≡	≡	≡	≡	≡	≡
2017-02-02 21:26:44	Google Chrome	Google Chrome	56.0.2924.87	Google Inc.	20170126		C:\Program Files (x86)\Google\Chrome\Appli cation	"C:\Program Files (x86)\Google\Chrome\Appli cation\56.0.2924.87\Installe r\setup.exe" --uninstall --system-level --verbose-logging	
2017-01-30 18:47:50	{FC965A47-4839-40CA-B618-18F486F042C6}	Skype™ 7.31	7.31.104	Skype Technologies S.A.	20170126	C:\ProgramData\Skype\{FC965A47-4839-40CA-B618-18F486F042C6}\	C:\Program Files (x86)\Skype\	MsiExec.exe /X {FC965A47-4839-40CA-B618-18F486F042C6}	
2017-01-27 02:47:49	{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005	12.0.21005	Microsoft Corporation	20151103	C:\ProgramData\Package Cache\F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185\vc12.0.21005\packages\vcRu ntimeAdditional_x86\		MsiExec.exe /X {F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	
2017-01-27 02:47:49	{f65db027-aff3-4070-886a-0d87064aabb1}	Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	12.0.30501.0	Microsoft Corporation				"C:\ProgramData\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcr edist_x86.exe" /uninstall	
2017-01-27 02:47:49	{F24F876B-7D71-4BD6-88E9-614D3B000044}	Alcor Micro Smart Card Reader Driver	1.7.44.0	Alcor Micro Corp.	20170126	c:\SWSETUP\DRV\InputDevi ces\AlcorMicro\AlcorMicr _LL NQB2\1.7.44.0\src\	c:\Program Files (x86)\AlcorMicro\	MsiExec.exe /X {F24F876B-7D71-4BD6-88E9-614D3B000044}	
2017-01-27 02:47:49	{F0E3AD40-28BD-4360-9C76-B9AC9A5886EA}	Intel(R) Processor Graphics	20.19.15.4331	Intel Corporation			C:\Program Files (x86)\Intel\Intel(R) Processor Graphics	"C:\Program Files (x86)\Intel\Intel(R) Processor Graphics\Uninstall\setup.ex e" -uninstall	
2017-01-27 02:47:49	{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573								

User Activities

- **Installed applications**
- **RecentDocs**
- **OpenSave MRU**
- **LastVisited MRU**
- **UserAssist**

Installed Applications

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\

Registry hives (5)				Available bookmarks (112/0)			
Enter text to search...				Find			
Key name	# values	# subkeys	Last write timestamp				
PenWorkspace	0	1	2017-01-27 02:43:58				
Policies	0	0	2017-01-27 02:43:59				
PrecisionTouchPad	11	1	2017-01-27 02:43:58				
PushNotifications	1	2	2017-02-02 21:24:17				
RADAR	2	0	2017-01-27 02:43:58				
Run	3	0	2017-02-02 22:25:27				
RunOnce	1	0	2017-02-01 16:55:27				
Screensavers	0	4	2017-01-27 02:43:58				
Search	14	4	2017-02-02 22:52:25				
Security and Maintenance	0	2	2017-01-27 16:59:07				
SettingSync	5	3	2017-01-27 02:52:38				
Shell Extensions	1	1	2017-01-27 16:54:37				
Skydrive	0	1	2017-01-27 16:57:07				
Store	0	4	2017-01-30 23:01:53				
Telephony	0	1	2017-01-27 02:43:58				
ThemeManager	11	0	2017-01-28 21:40:09				
Themes	11	2	2017-01-27 16:54:45				
UFH	0	1	2017-01-27 16:54:39				
Uninstall	0	3	2017-02-02 22:25:25				
OneDriveSetup.exe	10	0	2017-01-31 18:52:35				
Pidgin	7	0	2017-02-01 17:00:15				
yahoomessenger	13	0	2017-02-02 22:25:26				
WindowsUpdate	2	0	2017-02-02 21:29:17				

Values			
Drag a column header here to group by that column			
Value Name	Value Type	Data	Value Slack
DisplayIcon	RegSz	C:\Users\Sarah M\AppData\Lo...	
DisplayName	RegSz	Yahoo Messenger	A0-98-0A-00
DisplayVersion	RegSz	0.8.288	40-2B-87-D2
InstallDate	RegSz	20170202	0A-00
InstallLocation	RegSz	C:\Users\Sarah M\AppData\Lo...	
Publisher	RegSz	Yahoo! Inc	0A-00-48-95-0A-00
QuietUninstallString	RegSz	"C:\Users\Sarah M\AppData\Lo...	
UninstallString	RegSz	"C:\Users\Sarah M\AppData\Lo...	00-00-4D-00-69-00
URLUpdateInfo	RegSz	https://messenger.yahoo.com/	00-00
EstimatedSize	RegDword	44945	
NoModify	RegDword	1	
NoRepair	RegDword	1	
Language	RegDword	1033	

RecentDocs

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

Registry Explorer v1.6.0.0
File Tools Options Bookmarks (28/0) View Help
Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Package Installation	1	0	2017-01-27 17:13:25
RecentDocs	23	4	2017-02-02 22:52:25
.html	3	0	2017-02-02 22:52:25
.jpg	8	0	2017-02-02 22:38:25
.pdf	6	0	2017-02-02 22:39:08
Folder	6	0	2017-02-02 22:39:08
Ribbon	2	0	2017-01-27 17:19:25
RunMRU	0	0	2017-01-27 02:44:34
SearchPlatform	0	1	2017-01-27 02:43:58
Shell Folders	31	0	2017-01-27 16:54:48
Shutdown	1	0	2017-02-02 22:53:21
SoftLanding	2	0	2017-02-01 16:57:12
StartPage	3	0	2017-01-27 02:52:38
Streams	0	1	2017-01-27 02:52:38
StuckRects3	1	0	2017-01-27 02:52:38
Taskband	5	0	2017-02-02 22:49:01
TWinUI	0	1	2017-01-28 22:36:52
TypedPaths	0	0	2017-01-27 17:21:25
User Shell Folders	20	0	2017-01-27 02:44:00
UserAssist	0	9	2017-01-27 02:44:34
VirtualDesktops	0	0	2017-01-27 16:55:30
VisualEffects	0	19	2017-01-27 16:54:49
Wallpapers	7	0	2017-01-28 22:37:36
Ext	0	0	2017-01-27 02:52:39
FileAssociations	2	3	2017-01-27 16:55:26
FileHistory	0	1	2017-01-27 02:43:58

Values Recent documents

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted
MRUListEx	RegBinary	15-00-00-00-14-00-00-00-0E-00...		<input type="checkbox"/>
2	RegBinary	4C-00-75-00-6E-00-61-00-20-00...	C2-CB	<input type="checkbox"/>
4	RegBinary	47-00-72-00-65-00-61-00-74-00...	00-00	<input type="checkbox"/>
7	RegBinary	53-00-6E-00-6F-00-77-00-79-00...	00-00-00-00-00-00	<input type="checkbox"/>
8	RegBinary	50-00-79-00-67-00-6D-00-79-00...	00-00-00-00-00-00	<input type="checkbox"/>
6	RegBinary	47-00-72-00-65-00-61-00-74-00...	6F-00	<input type="checkbox"/>
5	RegBinary	70-00-65-00-74-00-73-00-00-00...	6B-00-00-00-18-00	<input type="checkbox"/>
0	RegBinary	6E-00-65-00-74-00-77-00-6F-00...	00-00-00-00-00-05	<input type="checkbox"/>
10	RegBinary	43-00-6F-00-6F-00-6C-00-20-00...	00-00-00-00-00-00	<input type="checkbox"/>
11	RegBinary	42-00-61-00-63-00-6B-00-67-00...		<input type="checkbox"/>
9	RegBinary	3F-00-4C-00-69-00-6E-00-6B-00...	63-00	<input type="checkbox"/>
1	RegBinary	54-00-68-00-65-00-20-00-49-00...	00-00-00-00-00-00	<input type="checkbox"/>
13	RegBinary	4F-00-77-00-6C-00-5F-00-4B-00...	00-00-00-00	<input type="checkbox"/>
3	RegBinary	44-00-6F-00-77-00-6E-00-6C-00...	00-00-00-00-00-00	<input type="checkbox"/>
16	RegBinary	4E-00-65-00-78-00-74-00-20-00...	00-00	<input type="checkbox"/>
17	RegBinary	4D-00-79-00-20-00-4E-00-65-00...		<input type="checkbox"/>
19	RegBinary	53-00-6E-00-6F-00-77-00-79-00...	00-00-00-00	<input type="checkbox"/>
15	RegBinary	53-00-6E-00-6F-00-77-00-79-00...	53-00-6E-00-6F-00	<input type="checkbox"/>
18	RegBinary	20-00-28-00-46-00-3A-00-29-00...	20-C7-06-00	<input type="checkbox"/>
12	RegBinary	4F-00-77-00-6C-00-5F-00-45-00...		<input type="checkbox"/>
14	RegBinary	4E-00-65-00-77-00-20-00-50-00...	30-00-41-00-34-00	<input type="checkbox"/>
20	RegBinary	57-00-4F-00-4C-00-66-00-20-00...	02-7F	<input type="checkbox"/>
21	RegBinary	77-00-68-00-61-00-74-00-20-00...	01-06-00-00	<input type="checkbox"/>

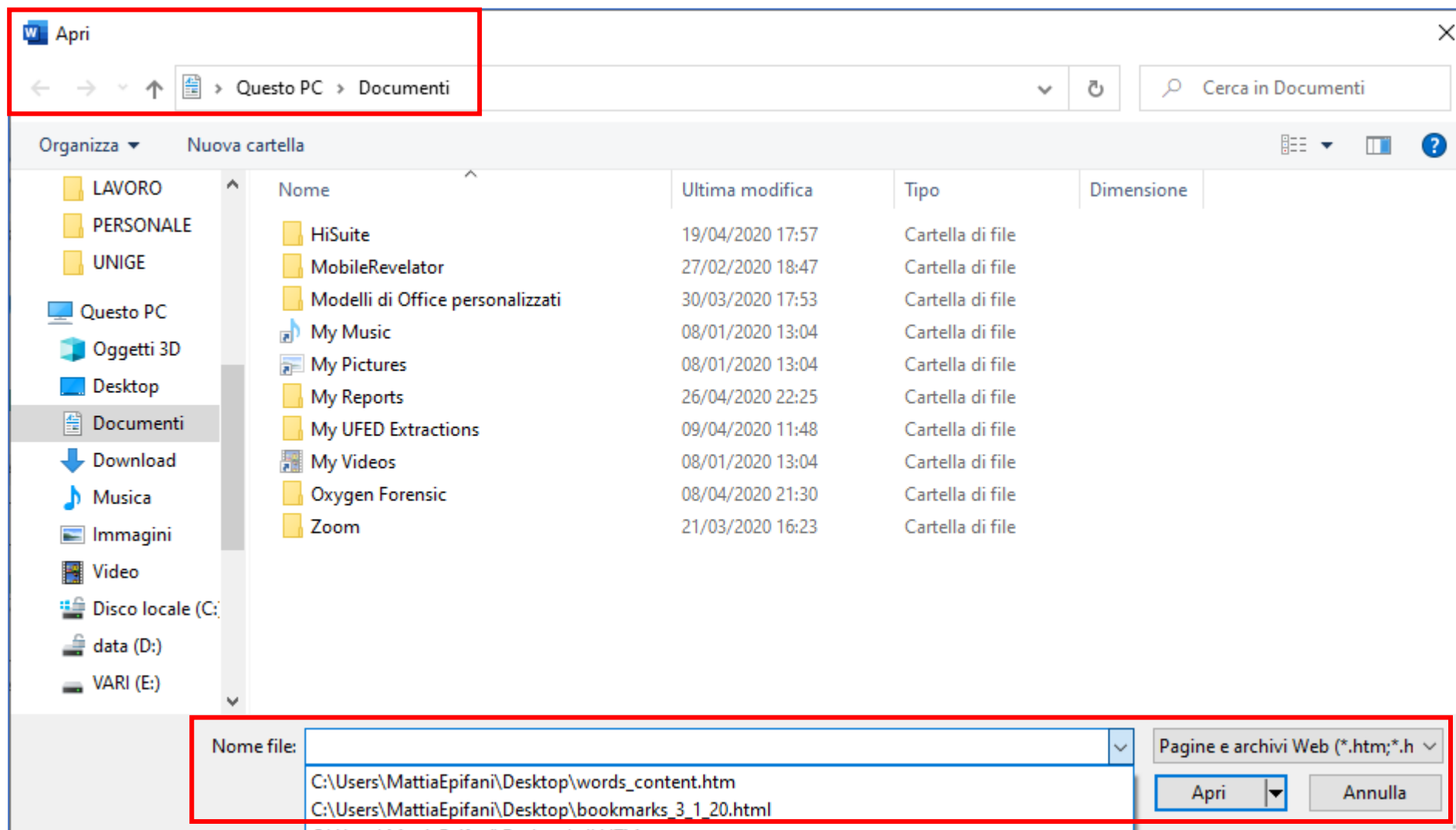
RecentDocs

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

Registry hives (5)				Available bookmarks (112/0)			
Enter text to search...				Find			
Key name	# values	# subkeys	Last write timestamp				
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	23	4	2017-02-02 22:52:25				
Package Installation	1	0	2017-01-27 17:13:29				
RecentDocs	23	4	2017-02-02 22:52:25				
.html	3	0	2017-02-02 22:52:25				
.jpg	8	0	2017-02-02 22:38:25				
.pdf	6	0	2017-02-02 22:39:08				
Folder	6	0	2017-02-02 22:39:08				
Ribbon	2	0	2017-01-27 17:13:29				
RunMRU	0	0	2017-01-27 02:44:34				
SearchPlatform	0	1	2017-01-27 02:43:58				
Shell Folders	31	0	2017-01-27 16:54:48				
Shutdown	1	0	2017-02-02 22:53:21				
SoftLanding	2	0	2017-02-01 16:57:12				
StartPage	3	0	2017-01-27 02:52:38				
Streams	0	1	2017-01-27 02:52:38				
StuckRects3	1	0	2017-01-27 02:52:38				
Taskband	5	0	2017-02-02 22:49:01				
TWinUI	0	1	2017-01-28 22:36:52				
TypedPaths	0	0	2017-01-27 17:21:25				
User Shell Folders	20	0	2017-01-27 02:44:00				
UserAssist	0	9	2017-01-27 02:44:34				
VirtualDesktops	0	0	2017-01-27 16:55:30				
VisualEffects	0	19	2017-01-27 16:54:49				
Wallpapers	7	0	2017-01-28 22:37:36				
Ext	0	0	2017-01-27 02:52:38				

Values Recent documents							
Drag a column header here to group by that column							
Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	=	=	=	
RecentDocs	21	what is this.html	what is this.lnk	0	2017-02-02 22:52:25	2017-02-02 22:52:25	
RecentDocs	20	WOLF Awsome.html	WOLF Awsome.lnk	1			
RecentDocs	14	New Pet Care	New Pet Care.lnk	2		2017-02-02 22:39:08	
RecentDocs	12	Owl_Emergency_Care.pdf	Owl_Emergency_Care.lnk	3		2017-02-02 22:39:08	
RecentDocs	18	(F:)	(F:).lnk	4			
RecentDocs	15	Snowy_Owl.pdf	Snowy_Owl.lnk	5			
RecentDocs	19	Snowy Owl Care.pdf	Snowy Owl Care.lnk	6			
RecentDocs	17	My New Pet.jpg	My New Pet.lnk	7		2017-02-02 22:38:25	
RecentDocs	16	Next pet	Next pet.lnk	8			
RecentDocs	3	Downloads	Downloads.lnk	9			
RecentDocs	13	Owl_Keeping.pdf	Owl_Keeping.lnk	10			
RecentDocs	1	The Internet	The Internet.lnk	11			
RecentDocs	9	?LinkId=219472&dclid=0x409	http--go.microsoft.com-fwlink-LinkID=219472&dclid=0x409.lnk	12			
RecentDocs	11	Background.jpg	Background.lnk	13			
RecentDocs	10	Cool picture of a tiger maybe wallhanging.jpg	Cool picture of a tiger maybe wallhanging.lnk	14			
RecentDocs	0	network-wifi	ms-settingsnetwork-wifi.lnk	15			
RecentDocs	5	pets	pets.lnk	16			
RecentDocs	6	Great Horned Owl.jpg	Great Horned Owl.lnk	17			
RecentDocs	8	Pygmy Owl.jpg	Pygmy Owl.lnk	18			
RecentDocs	7	Snowy Owl.jpg	Snowy Owl.lnk	19			
RecentDocs	4	Great Horned Owl Info.pdf	Great Horned Owl Info.lnk	20			

Common Dialog Box



LastVisited MRU

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

- For each executable, last path of file opened

Registry Explorer v1.5.2.0

File Tools Options Bookmarks (24/0) View Help

Registry hives (3) Available bookmarks (69/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
CIDSave	0	1	2020-01-08 18:18:11
CLSID	0	5	2020-01-08 12:04:47
ComDlg32	0	5	2020-02-12 10:17:05
CIDSizeMRU	56	0	2020-04-20 17:07:36
FirstFolder	7	0	2020-04-09 20:38:07
LastVisitedPidlMRU	26	0	2020-04-20 17:07:36
LastVisitedPidlMRULegacy	7	0	2020-04-19 17:28:12
OpenSavePidlMRU	0	42	2020-04-20 16:46:03
Desktop	0	1	2020-01-08 12:07:53
Discardable	0	1	2020-01-08 12:04:46
DiskSpaceChecking	5	0	2020-04-16 16:15:32
ExtractionWizard	1	0	2020-01-08 18:07:26
FeatureUsage	1	5	2020-01-09 08:23:16
FileExts	0	308	2020-04-18 13:58:07
HideDesktopIcons	0	1	2020-01-08 12:07:53
LogonStats	2	0	2020-01-08 12:04:45
LowRegistry	0	0	2020-01-08 12:04:46
MenuOrder	0	1	2020-01-08 12:04:46
MMStuckRects3	4	0	2020-03-09 19:57:11
Modules	0	3	2020-01-08 12:06:42

Values ComDlg32 LastVisitedPidlMRU

Drag a column header here to group by that column

Value Name	Mru Position	Executable	Absolute Path	Opened On
15	0	RegistryExplorer.exe	My Computer\D:\UNIGE_2020\Data_Leakage_Extracted	2020-04-20 17:07:36
13	1	FTK Imager.exe	My Computer\D:\UNIGE_2020\Data_Leakage	
7	2	SnippingTool.exe	My Computer\Desktop\INTERPOL_CNR_CATALOGUE	
5	3	chrome.exe	My Computer\Desktop\INTERPOL_CNR_CATALOGUE	

Total rows: 25

Type viewer Slack viewer

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Data interpreter ?

Value: MRUListEx Collapse all hives

Selected hive: ntuser.dat Last write: 2020-04-20 17:07:36 26 of 26 values shown (100,00%) Load complete Hidden keys: 0 19

OpenSave MRU

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

- For each extension, last files opened

Registry Explorer v1.5.2.0

File Tools Options Bookmarks (24/0) View Help

Registry hives (3) Available bookmarks (69/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Root	=	=	=
OpenSavePidlMRU	0	42	2020-04-20 16:46:03
*	21	0	2020-04-20 17:05:20
001	3	0	2020-04-20 09:28:01
apk	3	0	2020-03-15 10:55:12
bat	2	0	2020-04-04 11:08:13
bbb	9	0	2020-04-07 15:10:46
bin	21	0	2020-04-14 16:13:12
cer	3	0	2020-04-08 08:35:16
com	2	0	2020-03-17 11:05:02
cpkg	2	0	2020-02-28 16:03:30
DAT	7	0	2020-04-20 16:35:34
DAT_clean	2	0	2020-04-08 10:58:11
db	6	0	2020-03-14 17:08:52
docx	12	0	2020-04-16 18:15:12
E01	12	0	2020-04-20 14:28:26
Ex01	3	0	2020-04-02 15:58:02
exe	3	0	2020-02-27 14:50:43
htm	4	0	2020-03-14 17:12:01
html	2	0	2020-03-01 22:11:27

Values ComDlg32 OpenSavePidlMRU

Drag a column header here to group by that column

Extension	Value Name	Mru Position	Absolute Path	Opened On
exe	0	1	My Computer\Program Files\...	
htm	2	0	My Computer\Desktop\words_content.htm	2020-03-14 17:12:01
htm	1	1	My Computer\Desktop\all.HTM	
htm	0	2	all.htm	
html	0	0	My Computer\Desktop\bookmarks_3_1_2011...	2020-03-01 22:11:27

Total rows: 180

Type viewer

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

Value: None Collapse all hives

Selected hive: ntuser.dat Last write: 2020-04-20 16:46:03 Key contains no values Load complete Hidden keys: 0 19

Exercise 5

1. What is **the name of the last PDF** file opened by the **Sarah M** user?
2. When was the **My New Pet.jpg file** last opened by the **Sarah M** user?
3. When was the **Snowy_Owl.pdf** file last opened by the **Sarah M** user?
4. Which is the last folder used by the **Sarah M** user to **open/save files downloaded with Google Chrome** (chrome.exe)?

Exercise 5.1/5.2

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
HKEY_CURRENT_USER	=	=	=
MountPoints2	0	5	2017-02-02 21:53:09
Package Installation	1	0	2017-01-27 17:13:29
RecentDocs	23	4	2017-02-02 22:52:25
.html	3	0	2017-02-02 22:52:25
.jpg	8	0	2017-02-02 22:38:25
.pdf	6	0	2017-02-02 22:39:08
Folder	6	0	2017-02-02 22:39:08

Values Recent documents

Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
HKEY_CURRENT_USER	HKEY_CURRENT_USER	HKEY_CURRENT_USER	HKEY_CURRENT_USER	=	=
.pdf	1	Owl_Emergency_Care.pdf	Owl_Emergency_Care.lnk		0 2017-02-02 22:39:08
.pdf	3	Snowy_Owl.pdf	Snowy_Owl.lnk		1
.pdf	4	Snowy Owl Care.pdf	Snowy Owl Care.lnk		2
.pdf	2	Owl_Keeping.pdf	Owl_Keeping.lnk		3
.pdf	0	Great Horned Owl Info.pdf	Great Horned Owl Info.lnk		4

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
HKEY_CURRENT_USER	=	=	=
MountPoints2	0	5	2017-02-02 21:53:09
Package Installation	1	0	2017-01-27 17:13:29
RecentDocs	23	4	2017-02-02 22:52:25
.html	3	0	2017-02-02 22:52:25
.jpg	8	0	2017-02-02 22:38:25
.pdf	6	0	2017-02-02 22:39:08
Folder	6	0	2017-02-02 22:39:08
Ribbon	2	0	2017-01-27 17:19:25

Values Recent documents

Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
HKEY_CURRENT_USER	HKEY_CURRENT_USER	HKEY_CURRENT_USER	HKEY_CURRENT_USER	=	=
.jpg	6	My New Pet.jpg	My New Pet.lnk		0 2017-02-02 22:38:25
.jpg	5	Background.jpg	Background.lnk		1
.jpg	4	Cool picture of a tiger maybe wallhanging.jpg	Cool picture of a tiger maybe wallhanging.lnk		2
.jpg	1	Great Horned Owl.jpg	Great Horned Owl.lnk		3
.jpg	3	Pygmy Owl.jpg	Pygmy Owl.lnk		4
.jpg	2	Snowy Owl.jpg	Snowy Owl.lnk		5
.jpg	0	Luna Owl.jpg	Luna Owl.lnk		6

Exercise 5.3/5.4

Registry hives (5)				Available bookmarks (112/0)						
Enter text to search...				Find						
Key name	# values	# subkeys	Last write timestamp							
HKEY_CURRENT_USER	=	=	=							
MountPoints2	0	5	2017-02-02 21:53:09							
Package Installation	1	0	2017-01-27 17:13:29							
RecentDocs	23	4	2017-02-02 22:52:25							
.html	3	0	2017-02-02 22:52:25							
.jpg	8	0	2017-02-02 22:38:25							
.pdf	6	0	2017-02-02 22:39:08							
Folder	6	0	2017-02-02 22:39:08							
Ribbon	2	0	2017-01-27 17:19:25							
RunMRU	0	0	2017-01-27 02:44:34							
SearchPlatform	0	1	2017-01-27 02:43:58							
Shell Folders	31	0	2017-01-27 16:54:48							
Shutdown	1	0	2017-02-02 22:53:21							
SoftLanding	2	0	2017-02-01 16:57:12							
StartPage	3	0	2017-01-27 02:52:38							
Streams	0	1	2017-01-27 02:52:38							
StuckRects3	1	0	2017-01-27 02:52:38							

Values						
Recent documents						
Drag a column header here to group by that column						
Extension	Value Name	Target Name	Lnk Name	Mrp Position	Opened On	Extension Last Opened
HKEY_CURRENT_USER	HKEY_CURRENT_USER	HKEY_CURRENT_USER	HKEY_CURRENT_USER	=	=	=
RecentDocs	21	what is this.html	what is this.lnk	0	2017-02-02 22:52:25	2017-02-02 22:52:25
RecentDocs	20	WOLF Awsome.html	WOLF Awsome.lnk	1		
RecentDocs	14	New Pet Care	New Pet Care.lnk	2		2017-02-02 22:39:08
RecentDocs	12	Owl_Emergency_Care.pdf	Owl_Emergency_Care.lnk	3		2017-02-02 22:39:08
RecentDocs	18	(F:)	(F:).lnk	4		
RecentDocs	15	Snowy_Owl.pdf	Snowy_Owl.lnk	5		
RecentDocs	19	Snowy Owl Care.pdf	Snowy Owl Care.lnk	6		
RecentDocs	17	My New Pet.jpg	My New Pet.lnk	7		2017-02-02 22:38:25
RecentDocs	16	Next pet	Next pet.lnk	8		
RecentDocs	3	Downloads	Downloads.lnk	9		
RecentDocs	13	Owl_Keeping.pdf	Owl_Keeping.lnk	10		
RecentDocs	1	The Internet	The Internet.lnk	11		
RecentDocs	9	?LinkID=219472&dclid=0x409	http--go.microsoft.com-fwlink-LinkID=219472&dclid=0x409.lnk	12		
RecentDocs	11	Background.jpg	Background.lnk	13		

Registry hives (5)				Available bookmarks (112/0)						
Enter text to search...				Find						
Key name	# values	# subkeys	Last write timestamp							
HKEY_CURRENT_USER	=	=	=							
CIDOpen	0	1	2017-01-28 22:37:07							
CIDSave	0	1	2017-01-28 22:34:42							
CLSID	0	5	2017-01-27 02:45:02							
ComDlg32	0	4	2017-01-28 22:34:42							
CIDSizeMRU	3	0	2017-02-02 22:52:25							
FirstFolder	2	0	2017-01-31 19:14:57							
LastVisitedPidlMRU	3	0	2017-02-02 22:52:25							
OpenSavePidlMRU	0	4	2017-02-02 22:51:41							
*	10	0	2017-02-02 22:52:25							
html	3	0	2017-02-02 22:52:25							
jpg	4	0	2017-02-02 21:53:32							
pdf	4	0	2017-01-31 19:12:19							

Values				
ComDlg32 LastVisitedPidlMRU				
Drag a column header here to group by that column				
Value Name	Mrp Position	Executable	Absolute Path	Opened On
HKEY_CURRENT_USER	=	HKEY_CURRENT_USER	HKEY_CURRENT_USER	=
0	0	chrome.exe	My Computer\Desktop	2017-02-02 22:52:25
1	1	PickrHost.exe	My Computer\Downloads	

UserAssist (Executable)

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

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
MountPoints2	0	5	2017-02-02 21:53:09
Package Installation	1	0	2017-01-27 17:13:29
RecentDocs	23	4	2017-02-02 22:52:25
.html	3	0	2017-02-02 22:52:25
.jpg	8	0	2017-02-02 22:38:25
.pdf	6	0	2017-02-02 22:39:08
Folder	6	0	2017-02-02 22:39:08
Ribbon	2	0	2017-01-27 17:19:25
RunMRU	0	0	2017-01-27 02:44:34
SearchPlatform	0	1	2017-01-27 02:43:58
Shell Folders	31	0	2017-01-27 16:54:48
Shutdown	1	0	2017-02-02 22:53:21
SoftLanding	2	0	2017-02-01 16:57:12
StartPage	3	0	2017-01-27 02:52:38
Streams	0	1	2017-01-27 02:52:38
StuckRects3	1	0	2017-01-27 02:52:38
Taskband	5	0	2017-02-02 22:49:01
TWInUI	0	1	2017-01-28 22:36:52
TypedPaths	0	0	2017-01-27 17:21:25
User Shell Folders	20	0	2017-01-27 02:44:00
UserAssist	0	9	2017-01-27 02:44:34
{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}	1	1	2017-01-27 02:44:34
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}	1	1	2017-01-27 02:44:34
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}	1	1	2017-01-27 02:44:34
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}	1	1	2017-01-27 02:44:34
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	1	1	2017-01-27 02:44:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	2017-01-27 02:44:34
Count	13	0	2017-02-02 22:49:04

Values UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLCUACount:ctor	=	0	0d, 0h, 00m, 00s	
Microsoft.Getstarted_8wekyb3d8bbwe!App	14	21	0d, 0h, 07m, 00s	2017-01-27 00:33:27
UEME_CTLSESSION	152	348	0d, 7h, 33m, 01s	
Microsoft.Office.Sway_8wekyb3d8bbwe!Microsoft.Sway	13	19	0d, 0h, 06m, 15s	2017-01-27 00:33:27
Microsoft.WindowsMaps_8wekyb3d8bbwe!App	12	17	0d, 0h, 05m, 30s	2017-01-27 00:33:27
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	11	15	0d, 0h, 04m, 45s	2017-01-27 00:33:27
Microsoft.WindowsAlarms_8wekyb3d8bbwe!App	10	13	0d, 0h, 04m, 00s	2017-01-27 00:33:27
{System32}\SnippingTool.exe	9	11	0d, 0h, 03m, 15s	2017-01-27 00:33:27
{System32}\mspaint.exe	9	9	0d, 0h, 02m, 31s	2017-01-27 17:21:49
{System32}\notepad.exe	7	7	0d, 0h, 01m, 45s	2017-01-27 00:33:27
Microsoft.Windows.StickyNotes	6	5	0d, 0h, 01m, 00s	2017-01-27 00:33:27
{Windows}\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	0	9	0d, 0h, 01m, 31s	
windows.immersivecontrolpanel_cw5n1h2txyewy\microsoft.windows.immersivecontrolpanel	9	23	0d, 0h, 06m, 14s	2017-01-27 01:49:37
{Windows}\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe	0	37	0d, 0h, 22m, 49s	
Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge	3	10	0d, 0h, 02m, 10s	2017-02-01 17:21:10
{System32}\SystemSettingsBroker.exe	0	1	0d, 0h, 00m, 27s	

Total rows: 38

Type viewer Slack viewer

00000000 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D
0000001E FF FF FF FF 00
0000003C 80 BF 00 00 00 80 BF 00 00 00 80 BF 00 00 00 80 BF 00 00 00 80 BF 00 00 00 80 BF FF FF FF FF

UserAssist (Shortcut)

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

Registry hives (5)

Available bookmarks (112/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
<div> <div></div> <div>MountPoints2</div> </div>	0	5	2017-02-02 21:53:09
<div> <div></div> <div>Package Installation</div> </div>	1	0	2017-01-27 17:13:29
<div> <div></div> <div>RecentDocs</div> </div>	23	4	2017-02-02 22:52:25
<div> <div></div> <div>.html</div> </div>	3	0	2017-02-02 22:52:25
<div> <div></div> <div>.jpg</div> </div>	8	0	2017-02-02 22:38:25
<div> <div></div> <div>.pdf</div> </div>	6	0	2017-02-02 22:39:08
<div> <div></div> <div>Folder</div> </div>	6	0	2017-02-02 22:39:08
<div> <div></div> <div>Ribbon</div> </div>	2	0	2017-01-27 17:19:25
<div> <div></div> <div>RunMRU</div> </div>	0	0	2017-01-27 02:44:34
<div> <div></div> <div>SearchPlatform</div> </div>	0	1	2017-01-27 02:43:58
<div> <div></div> <div>Shell Folders</div> </div>	31	0	2017-01-27 16:54:48
<div> <div></div> <div>Shutdown</div> </div>	1	0	2017-02-02 22:53:21
<div> <div></div> <div>SoftLanding</div> </div>	2	0	2017-02-01 16:57:12
<div> <div></div> <div>StartPage</div> </div>	3	0	2017-01-27 02:52:38
<div> <div></div> <div>Streams</div> </div>	0	1	2017-01-27 02:52:38
<div> <div></div> <div>StuckRects3</div> </div>	1	0	2017-01-27 02:52:38
<div> <div></div> <div>Taskband</div> </div>	5	0	2017-02-02 22:49:01
<div> <div></div> <div>TWinUI</div> </div>	0	1	2017-01-28 22:36:52
<div> <div></div> <div>TypedPaths</div> </div>	0	0	2017-01-27 17:21:25
<div> <div></div> <div>User Shell Folders</div> </div>	20	0	2017-01-27 02:44:00
<div> <div></div> <div>UserAssist</div> </div>	0	9	2017-01-27 02:44:34
<div> <div></div> <div>{9E04CAB2-CC14-11DF-B88C-A2F1DED72085}</div> </div>	1	1	2017-01-27 02:44:34
<div> <div></div> <div>{A3D53349-6E61-4557-8FC7-0028EDCEE8F6}</div> </div>	1	1	2017-01-27 02:44:34
<div> <div></div> <div>{B267E3AD-A825-4A09-82B9-EEC22AA3B847}</div> </div>	1	1	2017-01-27 02:44:34
<div> <div></div> <div>{BCB48336-4DD0-48FF-BB0B-D3190DACB3E2}</div> </div>	1	1	2017-01-27 02:44:34
<div> <div></div> <div>{C4A39E8E-1738-42A8-9383-8A3A8B32193E}</div> </div>	1	1	2017-01-27 02:44:34
<div> <div></div> <div>{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}</div> </div>	1	1	2017-01-27 02:44:34
<div> <div></div> <div>Count</div> </div>	38	0	2017-02-02 22:53:21
<div> <div></div> <div>{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}</div> </div>	1	1	2017-01-27 02:44:34
<div> <div></div> <div>{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}</div> </div>	1	1	2017-01-27 02:44:34
<div> <div></div> <div>Count</div> </div>	13	0	2017-02-02 22:49:04

Values

UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s	
{Common Programs}\Accessories\Snipping Tool.lnk	9	0	0d, 0h, 00m, 00s	2017-01-27 00:33:27
UEME_CTLSESSION	77	0	0d, 0h, 00m, 00s	
{Common Programs}\Accessories\Paint.lnk	8	0	0d, 0h, 00m, 00s	2017-01-27 00:33:27
{Programs}\Accessories\Notepad.lnk	7	0	0d, 0h, 00m, 00s	2017-01-27 00:33:27
{Common Programs}\Accessories\Sticky Notes.lnk	6	0	0d, 0h, 00m, 00s	2017-01-27 00:33:27
{User Pinned}\TaskBar\Google Chrome.lnk	17	0	0d, 0h, 00m, 00s	2017-02-02 21:57:10
{User Pinned}\TaskBar\File Explorer.lnk	18	0	0d, 0h, 00m, 00s	2017-02-02 22:38:58
C:\Users\Public\Desktop\Skype.lnk	2	0	0d, 0h, 00m, 00s	2017-01-31 18:59:38
{Common Programs}\Skype\Skype.lnk	1	0	0d, 0h, 00m, 00s	2017-01-31 19:26:31
{Programs}\Pidgin.lnk	2	0	0d, 0h, 00m, 00s	2017-02-01 17:07:37
{User Pinned}\TaskBar\Pidgin.lnk	6	0	0d, 0h, 00m, 00s	2017-02-02 21:25:05
{User Pinned}\TaskBar\Yahoo Messenger.lnk	1	0	0d, 0h, 00m, 00s	2017-02-02 22:49:04

Total rows: 13

Export ?

Type viewer

Slack viewer

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D
00000000 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00
00000001E 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF

Exercise 6

1. When was the **Google Chrome** application **last executed** by the **Sarah M** user?
2. When was the **Skype** application **last executed** by the **Sarah M** user?
3. When was the **Pidgin** application **last executed** by the **Sarah M** user?
4. When was the **Yahoo Messenger** application **last executed** by the **Sarah M** user?
5. When was the **Google Chrome Setup** application **last executed** by the **Sarah M** user?

Exercise 6.1 / 6.2

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
HKLM\Software\Classes\CLSID\{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	1	1	2017-01-27 02:44:34
HKLM\Software\Classes\CLSID\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21

Values UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLSESSION	=	=	0d, 7h, 33m, 01s	=
Microsoft Windows Explorer	18	25	0d, 8h, 57m, 16s	2017-02-02 22:58:58
Chrome	17	69	0d, 4h, 28m, 48s	2017-02-02 21:57:10

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
HKLM\Software\Classes\CLSID\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21
HKLM\Software\Classes\CLSID\{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34
HKLM\Software\Classes\CLSID\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	2017-01-27 02:44:34
Count	13	0	2017-02-02 22:49:04

Values UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLSESSION	=	=	0d, 0h, 00m, 00s	=
{User Pinned}\TaskBar\{File Explorer.lnk}	18	0	0d, 0h, 00m, 00s	2017-02-02 22:38:58
{User Pinned}\TaskBar\{Google Chrome.lnk}	17	0	0d, 0h, 00m, 00s	2017-02-02 21:57:10
{Common Programs}\Accessories\Snipping Tool.lnk	9	0	0d, 0h, 00m, 00s	2017-01-27 00:33:27
{Common Programs}\Accessories\Paint.lnk	8	0	0d, 0h, 00m, 00s	2017-01-27 00:33:27

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
HKLM\Software\Classes\CLSID\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21
HKLM\Software\Classes\CLSID\{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34
HKLM\Software\Classes\CLSID\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	2017-01-27 02:44:34
Count	13	0	2017-02-02 22:49:04

Values UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
skype	=	=	0d, 0h, 00m, 17s	=
C:\Users\Sarah\M\Downloads\SkypeSetupFull.exe	0	1	0d, 0h, 00m, 17s	2017-01-31 19:26:31
Skype.Desktop.Application	3	18	0d, 0h, 22m, 35s	2017-01-31 19:26:31

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
HKLM\Software\Classes\CLSID\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21
HKLM\Software\Classes\CLSID\{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34
HKLM\Software\Classes\CLSID\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	2017-01-27 02:44:34
Count	13	0	2017-02-02 22:49:04

Values UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
skype	=	=	0d, 0h, 00m, 00s	=
C:\Users\Public\Desktop\Skype.lnk	2	0	0d, 0h, 00m, 00s	2017-01-31 18:59:38
{Common Programs}\Skype\Skype.lnk	1	0	0d, 0h, 00m, 00s	2017-01-31 19:26:31

Exercise 6.3 / 6.4

Registry hives (5)

Available bookmarks (112/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
HKLM\Software\Classes\CLSID\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21
HKLM\Software\Classes\CLSID\{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34
Count	13	0	2017-02-02 22:49:04
HKLM\Software\Classes\CLSID\{FA99DEC7-6AC2-453A-A5E2-5F28FF4507B0}	1	1	2017-01-27 02:44:34

Values

UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
C:\Users\Sarah\AppData\Local\Downloads\pidgin-2.11.0.exe	0	1	0d, 0h, 01m, 03s	
C:\Users\Sarah\AppData\Local\Roaming\Microsoft\Windows\Pidgin\pidgin.exe	8	12	0d, 1h, 08m, 22s	2017-02-02 21:25:05
C:\Users\Sarah\AppData\Local\Downloads\pidgin-2.11.0 (1).exe	0	1	0d, 0h, 00m, 05s	

Registry hives (5)

Available bookmarks (112/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
HKLM\Software\Classes\CLSID\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21
HKLM\Software\Classes\CLSID\{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34
Count	13	0	2017-02-02 22:49:04

Values

UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
{Programs}\Pidgin.Ink	2	0	0d, 0h, 00m, 00s	2017-02-01 17:07:37
{User Pinned}\TaskBar\Pidgin.Ink	6	0	0d, 0h, 00m, 00s	2017-02-02 21:25:05

Registry hives (5)

Available bookmarks (112/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
hikc	=	=	=
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	2017-01-27 02:44:34
Count	13	0	2017-02-02 22:49:04

Values

UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
hikc yah	=	=	hikc	=
com.squirrel.yahoomessenger.YahooMessenger	1	6	0d, 0h, 10m, 47s	2017-02-02 22:49:04

Registry hives (5)

Available bookmarks (112/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
HKLM\Software\Classes\CLSID\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34
Count	38	0	2017-02-02 22:53:21
HKLM\Software\Classes\CLSID\{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34
Count	1	1	2017-01-27 02:44:34
Count	13	0	2017-02-02 22:49:04

Values

UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
{User Pinned}\TaskBar\Yahoo Messenger.Ink	1	0	0d, 0h, 00m, 00s	2017-02-02 22:49:04

UniGe 2025 – DFIR – Windows

70

Exercise 6.5

Registry hives (5)					Available bookmarks (112/0)				
Enter text to search...					Find				
Key name	# values	# subkeys	Last write timestamp						
HKEY_CURRENT_USER									
Software\Classes\CLSID\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2017-01-27 02:44:34						
Count	38	0	2017-02-02 22:53:21						
Software\Classes\CLSID\{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2017-01-27 02:44:34						
Software\Classes\CLSID\{F4E57C4B-2036-45F0-A9AB-4438CFE33D9F}	1	1	2017-01-27 02:44:34						
Count	13	0	2017-02-02 22:49:04						
Software\Classes\CLSID\{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}	1	1	2017-01-27 02:44:34						
VirtualDesktops	0	0	2017-01-27 16:55:30						
VisualEffects	0	19	2017-01-27 16:54:49						
Wallpapers	7	0	2017-01-28 22:37:36						
Ext	0	0	2017-01-27 02:52:39						
FileAssociations	2	2	2017-01-27 16:55:36						

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
{Windows}\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	0	9	0d, 0h, 01m, 31s	
{Windows}\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe	0	37	0d, 0h, 22m, 49s	
C:\Users\Sarah M\AppData\Local\SquirrelTemp\Update.exe	0	1	0d, 0h, 00m, 04s	
C:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Pidgin\pidgin.exe	8	12	0d, 1h, 08m, 22s	2017-02-02 21:25:05
C:\Users\Sarah M\Downloads\ChromeSetup.exe	1	0	0d, 0h, 00m, 00s	2017-01-27 00:54:30
C:\Users\Sarah M\Downloads\pidgin-2.11.0 (1).exe	0	1	0d, 0h, 00m, 05s	
C:\Users\Sarah M\Downloads\pidgin-2.11.0.exe	0	1	0d, 0h, 01m, 03s	
C:\Users\Sarah M\Downloads\SkypeSetupFull.exe	0	1	0d, 0h, 00m, 17s	
Chrome	17	69	0d, 4h, 28m, 48s	2017-02-02 21:57:10
com.squirrel.yahoo.messenger.YahooMessenger	1	6	0d, 0h, 10m, 47s	2017-02-02 22:49:04

Evidence Tree		File List			
Sarah M		Name	Size	Type	Date Modified
AppData		ChromeSetup.exe	1,041	Regular File	27/01/2017 00:54:29
Application Data		SkypeSetupFull.exe	42,890	Regular File	27/01/2017 01:48:03
Contacts		desktop.ini	1	Regular File	27/01/2017 16:54:48
Cookies		Cool picture of a tiger maybe wallhangin...	18	Regular File	28/01/2017 22:34:42
Desktop		Background.jpg	10	Regular File	28/01/2017 22:36:41
Documents		Owl_Emergency_Care.pdf	140	Regular File	31/01/2017 19:09:01
Downloads		Owl_Keeping.pdf	214	Regular File	31/01/2017 19:09:11
Favorites		Bibliography - Snowy Owl 14 April 2014 - ...	388	Regular File	31/01/2017 19:12:44
IntelGraphicsProfiles		Sightings2005.xls	110	Regular File	31/01/2017 19:21:15
Links		pidgin-2.11.0.exe	9,040	Regular File	01/02/2017 16:59:37
Local Settings		pidgin-2.11.0 (1).exe	9,040	Regular File	01/02/2017 17:05:55
Music		yahoo-messenger-0.8.288-win32.exe	45,867	Regular File	02/02/2017 22:25:11
My Documents		1745.tmp		\$I30 INDX Entry	
NetHood					
OneDrive					
Pictures					
PrintHood					

LNK Files / Shortcut Files

- **Shell Item**: A data or a file containing information to access another file
- **LNK File/Shortcut**: a shell item saved in a file with LNK extension
 - A shortcut to execute an application on User's Desktop
 - A shortcut to open a file automatically created (recent file)
- A LNK file can contain
 - **Target drive type (Fixed, Removable, Network)**
 - **Path of target file**
 - Drive letter, volume label and volume serial number [LOCAL DRIVE]
 - Network path and drive letter (optional) [NETWORK RESOURCE]
 - **Target file MAC Timestamps**
 - **Target file size**

Recent Files

- **LNK Files** are automatically created by Windows in a “Recent folder”

- User based folder

%USERS%\<username>\AppData\Roaming\Microsoft\Windows\Recent

- For each non-executable opened file, the OS generates 2 LNK files
 - **Target file**
 - **Parent folder of target file**
- **149 files max** per user

Recent Files

- **LNK File Creation Time**

First time file by that name was opened

- **LNK File Modified Time**

Last time file by that name was opened

The screenshot displays a forensic analysis tool interface with three main panes: 'Evidence Tree', 'File List', and 'Properties'.

Evidence Tree: Shows a directory structure with folders like Hewlett-Packard, hpqLog, Intel, Intel Corporation, Microsoft, Credentials, Crypto, InputMethod, Internet Explorer, Network, Protect, Spelling, SystemCertificate, Vault, Windows, AccountPict, CloudStore, Libraries, Network Sho, Pidgin, Printer Short, Recent, Automati, CustomE, SendTo, Start Menu, and Templates.

File List: A table listing files with columns for Name, Size, Type, and Date Modified. The file 'Owl_Emergency_Care.Ink' is highlighted with a red box.

Name	Size	Type	Date Modified
CustomDestinations	1	Directory	02/02/2017 22:53:05
AutomaticDestinations	1	Directory	28/01/2017 22:37:09
what is this.Ink	1	Regular File	02/02/2017 22:52:25
\$I30	8	NTFS Index All...	02/02/2017 22:52:25
WOLF Awsome.Ink	1	Regular File	02/02/2017 22:51:41
New Pet Care.Ink	1	Regular File	02/02/2017 22:39:08
Owl_Emergency_Care.Ink	1	Regular File	02/02/2017 22:39:08
(F).Ink	1	Regular File	02/02/2017 22:38:39
Snowy_Owl.Ink	1	Regular File	02/02/2017 22:38:39
Snowy Owl Care.Ink	1	Regular File	02/02/2017 22:38:35
My New Pet.Ink	1	Regular File	02/02/2017 22:38:25
Next pet.Ink	1	Regular File	31/01/2017 19:27:24
Downloads.Ink	1	Regular File	31/01/2017 19:09:10
Owl_Keeping.Ink	1	Regular File	31/01/2017 19:09:10
The Internet.Ink	1	Regular File	30/01/2017 22:45:45
http--go.microsoft.com-fwlink-LinkID=2...	1	Regular File	30/01/2017 22:45:44
Background.Ink	1	Regular File	28/01/2017 22:36:41
Cool picture of a tiger maybe wallhangin...	1	Regular File	28/01/2017 22:34:42
ms-settingsnetwork-wifi.Ink	1	Regular File	28/01/2017 21:43:27
pets.Ink	1	Regular File	27/01/2017 17:23:32
Great Horned Owl.Ink	1	Regular File	27/01/2017 17:23:32
Pygmy Owl.Ink	1	Regular File	27/01/2017 17:23:29
Snowy Owl.Ink	1	Regular File	27/01/2017 17:23:25
desktop.ini	1	Regular File	27/01/2017 16:54:48
Great Horned Owl Info.Ink	1	Regular File	27/01/2017 01:16:48
Luna Owl.Ink	1	Regular File	27/01/2017 01:06:19

Properties: A table showing file metadata for 'Owl_Emergency_Care.Ink'. The 'Date Accessed', 'Date Created', and 'Date Modified' fields are highlighted with a red box.

Property	Value
Name	Owl_Emergency_Care.Ink
File Class	Regular File
File Size	865
Physical Size	4,096
Start Cluster	15,122,352
Date Accessed	02/02/2017 22:39:08
Date Created	31/01/2017 19:08:59
Date Modified	02/02/2017 22:39:08
Encrypted	False
Compressed	False
Actual File	True
Start Sector	121,980,288

DOS Attributes: A hex dump of the file's content. The path 'C:\Users\Sarah M\Documents\New Pet Care\Owl_Emergency_Care.pdf' is highlighted with a red box.

```
0f0 20 00 43 00 61 00 72 00-65 00 00 00 18 00 7A 00  C-a-r-e-...z-
100 32 00 C6 2C 02 00 3F 4A-21 99 20 00 4F 57 4C 5F 2-E, -?J!- -OWL_
110 45 4D 7E 31 2E 50 44 46-00 00 5E 00 09 00 04 00 EM~1.PDF-^.....
120 EF BE 3F 4A 44 99 3F 4A-44 99 2E 00 00 00 21 41 i%?JD-?JD-...!A
130 02 00 00 00 09 00 00 00-00 00 00 00 00 00 00 00 .....
140 00 00 00 00 E6 D1 3E 00-4F 00 77 00 6C 00 5F 00 ....aÑ>-O-w-l_-
150 45 00 6D 00 65 00 72 00-67 00 65 00 6E 00 63 00 E-m-e-r-g-e-n-c-
160 79 00 5F 00 43 00 61 00-72 00 65 00 2E 00 70 00 y_-C-a-r-e-.p-
170 64 00 66 00 00 00 1C 00-00 00 74 00 00 00 1C 00 d-f-...t-...
180 00 00 01 00 00 1C 00-00 00 34 00 00 00 00 00 00 .....4.....
190 00 00 73 00 00 00 18 00-00 00 03 00 00 00 37 25 ...s...../s
1a0 41 14 10 00 00 00 57 69-6E 64 6F 77 73 00 43 32 A-...-Windows-C:
1b0 5C 55 73 65 72 73 5C 53-61 72 61 68 20 4D 5C 44 \Users\Sarah M\
1c0 6F 63 75 6D 65 6E 74 73-5C 4E 65 77 20 65 74 oments\New Pet
1d0 20 43 61 72 65 5C 4F 77-6C 5F 45 6D 65 72 67 65 Care\Owl_Emer
1e0 6E 63 79 5F 43 61 72 65-2E 70 64 66 00 00 3C 00 ncy_Care.pdf-<-
```

Recent Files

- **LNK File Creation Time**

First time file by that name was opened

- **LNK File Modified Time**

Last time file by that name was opened

The screenshot displays a Windows Explorer window with the 'Recent' folder selected in the left-hand pane. The right-hand pane shows a list of files, with 'Snowy_Owl.Ink' highlighted. Below the file list, the 'Properties' window is open, showing details for 'Snowy_Owl.Ink'. The 'Date Created' and 'Date Modified' fields are highlighted with a red box, showing '31/01/2017 19:12:19' and '02/02/2017 22:38:39' respectively. The 'DOS Attributes' section shows the file is not hidden, not a system file, and not read-only. The 'Actual File' section shows the file is a symbolic link to 'Snowy_Owl.pdf' in the 'F:\Snowy_Owl' directory.

Name	Size	Type	Date Modified
CustomDestinations	1	Directory	02/02/2017 22:53:05
AutomaticDestinations	1	Directory	28/01/2017 22:37:09
what is this.Ink	1	Regular File	02/02/2017 22:52:25
\$I30	8	NTFS Index All...	02/02/2017 22:52:25
WOLF Awsome.Ink	1	Regular File	02/02/2017 22:51:41
New Pet Care.Ink	1	Regular File	02/02/2017 22:39:08
Owl_Emergency_Care.Ink	1	Regular File	02/02/2017 22:39:08
(F).Ink	1	Regular File	02/02/2017 22:38:39
Snowy_Owl.Ink	1	Regular File	02/02/2017 22:38:39
Snowy Owl Care.Ink	1	Regular File	02/02/2017 22:38:39
My New Pet.Ink	1	Regular File	02/02/2017 22:38:25
Next pet.Ink	1	Regular File	31/01/2017 19:27:24
Downloads.Ink	1	Regular File	31/01/2017 19:09:10
Owl_Keeping.Ink	1	Regular File	31/01/2017 19:09:10
The Internet.Ink	1	Regular File	30/01/2017 22:45:45
http--go.microsoft.com-fwlink-LinkID=2...	1	Regular File	30/01/2017 22:45:44
Background.Ink	1	Regular File	28/01/2017 22:36:41
Cool picture of a tiger maybe wallhangin...	1	Regular File	28/01/2017 22:34:42
ms-settingsnetwork-wifi.Ink	1	Regular File	28/01/2017 21:43:27
pets.Ink	1	Regular File	27/01/2017 17:23:32
Great Horned Owl.Ink	1	Regular File	27/01/2017 17:23:32
Pygmy Owl.Ink	1	Regular File	27/01/2017 17:23:29
Snowy Owl.Ink	1	Regular File	27/01/2017 17:23:25
desktop.ini	1	Regular File	27/01/2017 16:54:48
Great Horned Owl Info.Ink	1	Regular File	27/01/2017 01:16:48
Luna Owl.Ink	1	Regular File	27/01/2017 01:06:19

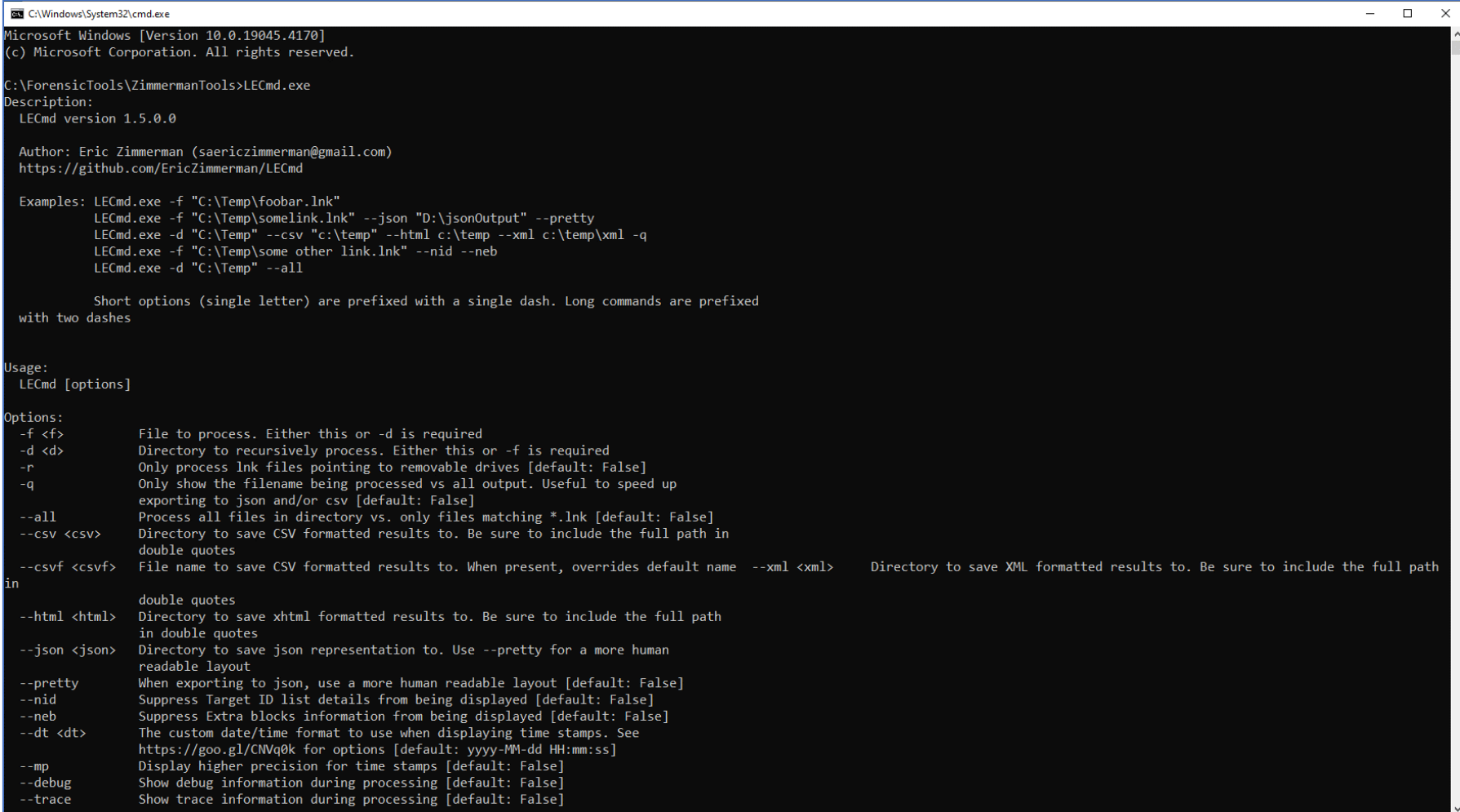
Name	File Class	File Size	Physical Size	Date Accessed	Date Created	Date Modified	Encrypted	Compressed	Actual File
Snowy_Owl.Ink	Regular File	344	344	02/02/2017 22:38:39	31/01/2017 19:12:19	02/02/2017 22:38:39	False	False	True

DOS Attributes	
8.3 Short Filename	SNOWY_~1.LNK
Hidden	False
System	False
Read only	False
Archive	True

```
000 4C 00 00 00 01 14 02 00-00 00 00 00 C0 00 00 00 L.....Ã...
010 00 00 00 46 93 00 20 00-20 00 00 00 20 74 02 D7 ...F... ..t..*
020 9F 7D D2 01 00 C8 BE 34-11 7D D2 01 00 99 AD 54 ..}ð--È%4-}ð---T
030 F6 7B D2 01 71 0D 09 00-00 00 00 00 01 00 00 00 8{ð-q.....
040 00 00 00 00 00 00 00 00-00 00 00 00 BF 00 55 00 ..-/...!ð-/F:\..
050 1F 00 2F 00 10 B7 A6 F5-19 00 2F 46 3A 5C 00 00 ..-/...!ð-/F:\..
060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..-/...!ð-/F:\..
070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..-/...!ð-/F:\..
080 00 00 00 74 1A 59 5E 96-DF D3 48 8D 67 17 33 BC ...t-Y^BÔH-g-3%
090 EE 28 BA 77 2C FB F5 2F-0E 16 4A A3 81 3E 56 0C î(*w,ûð/-..JÊ->V
0a0 68 BC 83 68 00 32 00 71-0D 09 00 3F 4A E3 99 20 h%h-2-q-...?JÃ·
0b0 00 53 4E 4F 57 59 5F 7E-31 2E 50 44 46 00 00 4C ·SNOWY_~1.PDF·L
0c0 00 09 00 04 00 EF BE 42-4A 21 B0 42 4A 00 28 2E ....i%Bj!*BJ·(.
0d0 00 00 00 C0 83 39 00 00-00 00 00 00 00 00 00 00 ...À-9.....
0e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....S-n
0f0 00 6F 00 77 00 79 00 5F-00 4F 00 77 00 6C 00 2E ·o-w-y-·O-w-l·
100 00 70 00 64 00 66 00 00-00 1C 00 00 00 3F 00 00 ·p-d-f-...?·
110 00 1C 00 00 00 01 00 00-00 1C 00 00 00 2D 00 00 .....>.....
120 00 00 00 00 00 3E 00 00-00 11 00 00 00 02 00 00 .....>.....
130 00 A2 89 BC 80 10 00 00-00 00 46 3A 5C 53 6E 67 ·e-Å-...F:\Sno
140 77 79 5F 4F 77 6C 2E 70-64 66 00 00 03 00 46 00 wy_Owl.pdf···F·
150 3A 00 5C 00 00 00 00 00-00
```

Parsing LNK

- **LECcmd** by Eric Zimmerman



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\ForensicTools\ZimmermanTools>LECcmd.exe
Description:
  LECmd version 1.5.0.0

  Author: Eric Zimmerman (saericzimmerman@gmail.com)
  https://github.com/EricZimmerman/LECcmd

  Examples: LECmd.exe -f "C:\Temp\foobar.lnk"
            LECmd.exe -f "C:\Temp\somelink.lnk" --json "D:\jsonOutput" --pretty
            LECmd.exe -d "C:\Temp" --csv "c:\temp" --html c:\temp --xml c:\temp\xml -q
            LECmd.exe -f "C:\Temp\some other link.lnk" --nid --neb
            LECmd.exe -d "C:\Temp" --all

  Short options (single letter) are prefixed with a single dash. Long commands are prefixed
  with two dashes

Usage:
  LECmd [options]

Options:
  -f <f>      File to process. Either this or -d is required
  -d <d>      Directory to recursively process. Either this or -f is required
  -r          Only process lnk files pointing to removable drives [default: False]
  -q          Only show the filename being processed vs all output. Useful to speed up
             exporting to json and/or csv [default: False]
  --all       Process all files in directory vs. only files matching *.lnk [default: False]
  --csv <csv> Directory to save CSV formatted results to. Be sure to include the full path in
             double quotes
  --csvf <csvf> File name to save CSV formatted results to. When present, overrides default name
in             double quotes
  --html <html> Directory to save xhtml formatted results to. Be sure to include the full path
             in double quotes
  --json <json> Directory to save json representation to. Use --pretty for a more human
             readable layout
  --pretty    When exporting to json, use a more human readable layout [default: False]
  --nid       Suppress Target ID list details from being displayed [default: False]
  --neb       Suppress Extra blocks information from being displayed [default: False]
  --dt <dt>   The custom date/time format to use when displaying time stamps. See
             https://goo.gl/CNVq0k for options [default: yyyy-MM-dd HH:mm:ss]
  --mp        Display higher precision for time stamps [default: False]
  --debug     Show debug information during processing [default: False]
  --trace     Show trace information during processing [default: False]
```

Parsing a single LNK file

- **Lecmd.exe -f "filename.lnk"**

```
C:\Windows\System32\cmd.exe
C:\ForensicTools\ZimmermanTools>lecmd -f "E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Owl_Emergency_Care.lnk"
LECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Owl_Emergency_Care.lnk

Warning: Administrator privileges not found!

Processing E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Owl_Emergency_Care.lnk
Source file: E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Owl_Emergency_Care.lnk
Source created: 2017-01-31 19:08:59
Source modified: 2017-02-02 22:39:08
Source accessed: 2024-04-05 11:33:26

--- Header ---
Target created: 2017-01-31 19:10:07
Target modified: 2017-01-31 19:09:01
Target accessed: 2017-01-31 19:10:07

File size (bytes): 142,534
Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode, DisableKnownFolderTracking
File attributes: FileAttributeArchive
Icon index: 0
Show window: SwNormal (Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.)

Relative Path: ..\..\..\..\Documents\New Pet Care\Owl_Emergency_Care.pdf
Working Directory: C:\Users\Sarah M\Documents\New Pet Care
```

Parsing a single LNK file

- **Lecmd.exe -f "filename.lnk"**

```
C:\Windows\System32\cmd.exe
Relative Path: ..\..\..\..\Documents\New Pet Care\Owl_Emergency_Care.pdf
Working Directory: C:\Users\Sarah M\Documents\New Pet Care

--- Link information ---
Flags: VolumeIdAndLocalBasePath

> Volume information
Drive type: Fixed storage media (Hard drive)
Serial number: 14412537
Label: Windows
Local path: C:\Users\Sarah M\Documents\New Pet Care\Owl_Emergency_Care.pdf

--- Target ID information (Format: Type ==> Value) ---

Absolute path: My Computer\Documents\New Pet Care\Owl_Emergency_Care.pdf

-Root folder: GUID ==> My Computer

-Root folder: GUID ==> Documents

-Directory ==> New Pet Care
Short name: NEWPET~1
Modified: 2017-02-02 22:00:36
Extension block count: 1

----- Block 0 (Beef0004) -----
Long name: New Pet Care
Created: 2017-01-31 19:09:26
Last access: 2017-02-02 22:00:36
MFT entry/sequence #: 154315/14 (0x25ACB/0xE)
```

Parsing a folder

- **Lecmd.exe -d <PATH-TO-FOLDER> --csv <PATH-TO-OUTPUT>**

```
C:\Windows\System32\cmd.exe
C:\ForensicTools\ZimmermanTools>lecmd -d "E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent" --csv D:\UNIGE
LECmd version 1.5.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd
Command line: -d E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent --csv D:\UNIGE
Warning: Administrator privileges not found!


Looking for lnk files in E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent
Found 22 files
Processing E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\ (F).lnk

Source file: E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\ (F).lnk
Source created: 2017-02-02 21:53:32
Source modified: 2017-02-02 22:38:39
Source accessed: 2024-04-05 11:37:53

--- Header ---
Target created: 1980-01-01 05:00:00
Target modified: 1980-01-01 05:00:00
Target accessed: 1980-01-01 05:00:00

File size (bytes): 0
Flags: HasTargetIdList, HasLinkInfo, IsUnicode, DisableKnownFolderTracking
File attributes: FileAttributeDirectory
```


Parsing a folder

(D:) > UNIGE > EXTRACTED				
	Name	Date modified	Type	Size
	 20240405113753_LECmd_Output.csv	05/04/2024 13:39	CSV File	11 KB



Line	Tag	Source File	Source Created	Source Modified	Target Created	Target Modified
7	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\http--go.microsoft.com-fwlink-LinkID=219472&clid=0x409.lnk	2017-01-28 21:41:16	2017-01-30 22:45:44		
9	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\ms-settingsnetwork-wifi.lnk	2017-01-27 00:45:10	2017-01-28 21:43:27		
20	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\The Internet.lnk	2017-01-27 00:45:11	2017-01-30 22:45:45		
2	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Background.lnk	2017-01-28 22:36:41	2017-01-28 22:36:41		
3	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Cool picture of a tiger maybe wallhanging.lnk	2017-01-28 22:34:42	2017-01-28 22:34:42		
4	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk	2017-01-27 01:06:20	2017-01-31 19:09:10	2017-01-27 00:34:48	2017-01-31 19:09:10
5	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Great Horned Owl Info.lnk	2017-01-27 01:16:48	2017-01-27 01:16:48		
6	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Great Horned Owl.lnk	2017-01-27 17:21:49	2017-01-27 17:23:32	2017-01-27 17:19:12	2017-01-27 17:19:12
8	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Luna Owl.lnk	2017-01-27 01:06:19	2017-01-27 01:06:19		
11	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\New Pet Care.lnk	2017-01-31 19:10:23	2017-02-02 22:39:08	2017-01-31 19:09:25	2017-02-02 22:00:34
12	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Next pet.lnk	2017-01-31 19:27:24	2017-01-31 19:27:24		
13	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Owl_Emergency_Care.lnk	2017-01-31 19:08:59	2017-02-02 22:39:08	2017-01-31 19:10:07	2017-01-31 19:09:01
14	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Owl_Keeping.lnk	2017-01-31 19:09:10	2017-01-31 19:09:10		
15	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\pets.lnk	2017-01-27 17:20:08	2017-01-27 17:23:32	2017-01-27 17:19:59	2017-01-27 17:20:24
16	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Pygmy Owl.lnk	2017-01-27 17:23:29	2017-01-27 17:23:29	2017-01-27 17:19:14	2017-01-27 17:19:16
18	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Snowy Owl.lnk	2017-01-27 17:23:25	2017-01-27 17:23:25	2017-01-27 17:19:16	2017-01-27 17:19:18
21	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\what is this.lnk	2017-02-02 22:52:25	2017-02-02 22:52:25		
22	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\WOLf Awsome.lnk	2017-02-02 22:51:41	2017-02-02 22:51:41		
1	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\ (F).lnk	2017-02-02 21:53:32	2017-02-02 22:38:39	1980-01-01 05:00:00	1980-01-01 05:00:00
10	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\My New Pet.lnk	2017-02-02 21:53:32	2017-02-02 22:38:25	2017-02-02 21:37:40	2017-02-02 21:37:30
17	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Snowy Owl Care.lnk	2017-02-02 22:38:35	2017-02-02 22:38:35	2017-02-02 21:38:22	2017-02-02 21:38:12
19	<input type="checkbox"/>	E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\Snowy_Owl.lnk	2017-01-31 19:12:19	2017-02-02 22:38:39	2017-02-02 22:01:00	2017-01-31 19:15:06

Exercise 7

1. When was the **Great Horned Owl Info.pdf** file first opened by the **Sarah M** user?
2. What is the file size (in bytes) of the **My New Pet.jpg** file?
3. When was the **Owl_Emergency_Care.pdf** file opened for the **first** time by the **Sarah M** user?
4. When was the **Owl_Emergency_Care.pdf** file opened for the **last** time by the **Sarah M** user?
5. Which files were opened from a **USB Drive**?
6. What is the **Volume Serial Number** of the USB Drive?

Exercise 7.1 / 7.2 / 7.3 / 7.4

20240405204358_LECmd_Output.csv

Drag a column header here to group by that column

Enter text to search...

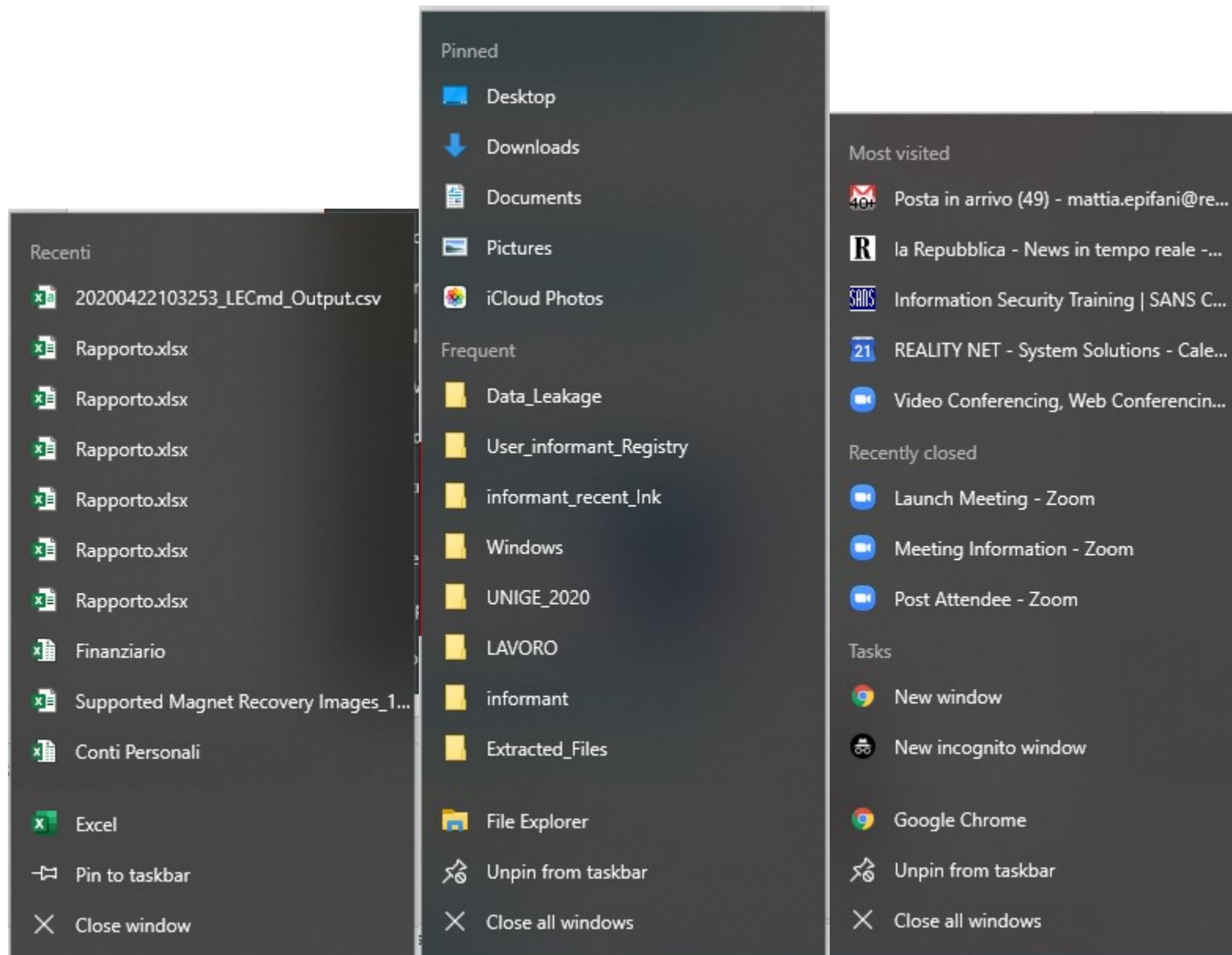
	Line	Tag	Source F...	Source Created	Source Modified	Target Created	Target Modified	Target Access...	File Si...	Local Path
T	=			=	=	=	=	=	=	
▶	1	<input type="checkbox"/>	E:\Users...	2017-02-02 21:53:32	2017-02-02 22:38:39	1980-01-01 05:00:00	1980-01-01 05:00:00	1980-01-01 05...	0	F:\
	2	<input type="checkbox"/>	E:\Users...	2017-01-28 22:36:41	2017-01-28 22:36:41				0	C:\Users\Sarah M\Downloads\Background.jpg
	3	<input type="checkbox"/>	E:\Users...	2017-01-28 22:34:42	2017-01-28 22:34:42				0	C:\Users\Sarah M\Downloads\Cool picture of a tiger maybe wallhanging.jpg
	4	<input type="checkbox"/>	E:\Users...	2017-01-27 01:06:20	2017-01-31 19:09:10	2017-01-27 00:34:48	2017-01-31 19:09:10	2017-01-31 19...	4096	C:\Users\Sarah M\Downloads
	5	<input type="checkbox"/>	E:\Users...	2017-01-27 01:16:48	2017-01-27 01:16:48				0	C:\Users\Sarah M\Downloads\Great Horned Owl Info.pdf
	6	<input type="checkbox"/>	E:\Users...	2017-01-27 17:21:49	2017-01-27 17:23:32	2017-01-27 17:19:12	2017-01-27 17:19:12	2017-01-27 17...	64476	C:\Users\Sarah M\Desktop\pets\Great Horned Owl.jpg
	7	<input type="checkbox"/>	E:\Users...	2017-01-28 21:41:16	2017-01-30 22:45:44				0	
	8	<input type="checkbox"/>	E:\Users...	2017-01-27 01:06:19	2017-01-27 01:06:19				0	C:\Users\Sarah M\Downloads\Luna Owl.jpg
	9	<input type="checkbox"/>	E:\Users...	2017-01-27 00:45:10	2017-01-28 21:43:27				0	
	10	<input type="checkbox"/>	E:\Users...	2017-02-02 21:53:32	2017-02-02 22:38:25	2017-02-02 21:37:40	2017-02-02 21:37:30	2017-02-02 05...	58248	F:\My New Pet.jpg
	11	<input type="checkbox"/>	E:\Users...	2017-01-31 19:10:23	2017-02-02 22:39:08	2017-01-31 19:09:25	2017-02-02 22:00:34	2017-02-02 22...	4096	C:\Users\Sarah M\Documents\New Pet Care
	12	<input type="checkbox"/>	E:\Users...	2017-01-31 19:27:24	2017-01-31 19:27:24				0	C:\Users\Sarah M\Desktop\Next pet
	13	<input type="checkbox"/>	E:\Users...	2017-01-31 19:08:59	2017-02-02 22:39:08	2017-01-31 19:10:07	2017-01-31 19:09:01	2017-01-31 19...	142534	C:\Users\Sarah M\Documents\New Pet Care\Owl_Emergency_Care.pdf
	14	<input type="checkbox"/>	E:\Users...	2017-01-31 19:09:10	2017-01-31 19:09:10				0	C:\Users\Sarah M\Downloads\Owl_Keeping.pdf
	15	<input type="checkbox"/>	E:\Users...	2017-01-27 17:20:08	2017-01-27 17:23:32	2017-01-27 17:19:59	2017-01-27 17:20:24	2017-01-27 17...	4096	C:\Users\Sarah M\Desktop\pets
	16	<input type="checkbox"/>	E:\Users...	2017-01-27 17:23:29	2017-01-27 17:23:29	2017-01-27 17:19:14	2017-01-27 17:19:16	2017-01-27 17...	94519	C:\Users\Sarah M\Desktop\pets\Pygmy Owl.jpg
	17	<input type="checkbox"/>	E:\Users...	2017-02-02 22:38:35	2017-02-02 22:38:35	2017-02-02 21:38:22	2017-02-02 21:38:12	2017-02-02 05...	593265	F:\Snowy Owl Care.pdf
	18	<input type="checkbox"/>	E:\Users...	2017-01-27 17:23:25	2017-01-27 17:23:25	2017-01-27 17:19:16	2017-01-27 17:19:18	2017-01-27 17...	5948982	C:\Users\Sarah M\Desktop\pets\Snowy Owl.jpg
	19	<input type="checkbox"/>	E:\Users...	2017-01-31 19:12:19	2017-02-02 22:38:39	2017-02-02 22:01:00	2017-01-31 19:15:06	2017-02-02 05...	593265	F:\Snowy_Owl.pdf
	20	<input type="checkbox"/>	E:\Users...	2017-01-27 00:45:11	2017-01-30 22:45:45				0	
	21	<input type="checkbox"/>	E:\Users...	2017-02-02 22:52:25	2017-02-02 22:52:25				0	C:\Users\Sarah M\Desktop\what is this.html
	22	<input type="checkbox"/>	E:\Users...	2017-02-02 22:51:41	2017-02-02 22:51:41				0	C:\Users\Sarah M\Desktop\WOLf Awsome.html

Exercise 7.5 / 7.6

20240405204358_LECmd_Output.csv						
Drag a column header here to group by that column						
Enter text to search... Find						
et Acce...	File Si...	Local Path	Target ID Absolute Path	Volume Serial Number	Drive Type	Volume Label
	=	C:	C:	C:	C:	C:
	0		Internet Explorer (Homepage)\http://go.microsoft.c...		(None)	
	0		Internet Explorer (Homepage)\ms-settings:network-w...		(None)	
	0		Internet Explorer (Homepage)		(None)	
	0	C:\Users\Sarah M\Downloads\Background.jpg	My Computer\Downloads\Background.jpg	14412537	Fixed storage media (Hard...	Windows
	0	C:\Users\Sarah M\Downloads\Cool picture of a tiger maybe wallhanging.jpg	My Computer\Downloads\Cool picture of a tiger mayb...	14412537	Fixed storage media (Hard...	Windows
-01-31 19...	4096	C:\Users\Sarah M\Downloads	My Computer\Downloads	14412537	Fixed storage media (Hard...	Windows
	0	C:\Users\Sarah M\Downloads\Great Horned Owl Info.pdf	My Computer\Downloads\Great Horned Owl Info.pdf	14412537	Fixed storage media (Hard...	Windows
-01-27 17...	64476	C:\Users\Sarah M\Desktop\pets\Great Horned Owl.jpg	My Computer\Desktop\pets\Great Horned Owl.jpg	14412537	Fixed storage media (Hard...	Windows
	0	C:\Users\Sarah M\Downloads\Luna Owl.jpg	My Computer\Downloads\Luna Owl.jpg	14412537	Fixed storage media (Hard...	Windows
-02-02 22...	4096	C:\Users\Sarah M\Documents\New Pet Care	My Computer\Documents\New Pet Care	14412537	Fixed storage media (Hard...	Windows
	0	C:\Users\Sarah M\Desktop\Next pet	My Computer\Desktop\Next pet	14412537	Fixed storage media (Hard...	Windows
-01-31 19...	142534	C:\Users\Sarah M\Documents\New Pet Care\Owl_Emergency_Care.pdf	My Computer\Documents\New Pet Care\Owl_Emergency_C...	14412537	Fixed storage media (Hard...	Windows
	0	C:\Users\Sarah M\Downloads\Owl_Keeping.pdf	My Computer\Downloads\Owl_Keeping.pdf	14412537	Fixed storage media (Hard...	Windows
-01-27 17...	4096	C:\Users\Sarah M\Desktop\pets	My Computer\Desktop\pets	14412537	Fixed storage media (Hard...	Windows
-01-27 17...	94519	C:\Users\Sarah M\Desktop\pets\Pygmy Owl.jpg	My Computer\Desktop\pets\Pygmy Owl.jpg	14412537	Fixed storage media (Hard...	Windows
-01-27 17...	5948982	C:\Users\Sarah M\Desktop\pets\Snowy Owl.jpg	My Computer\Desktop\pets\Snowy Owl.jpg	14412537	Fixed storage media (Hard...	Windows
	0	C:\Users\Sarah M\Desktop\what is this.html	My Computer\Desktop\what is this.html	14412537	Fixed storage media (Hard...	Windows
	0	C:\Users\Sarah M\Desktop\WOLf Awsome.html	My Computer\Desktop\WOLf Awsome.html	14412537	Fixed storage media (Hard...	Windows
-01-01 05...	0	F:\	F:	80BC89A2	Removable storage media (
-02-02 05...	58248	F:\My New Pet.jpg	F:\My New Pet.jpg	80BC89A2	Removable storage media (...)	
-02-02 05...	593265	F:\Snowy Owl Care.pdf	F:\Snowy Owl Care.pdf	80BC89A2	Removable storage media (...)	
-02-02 05...	593265	F:\Snowy_Owl.pdf	F:\Snowy_Owl.pdf	80BC89A2	Removable storage media (...)	

Jumplists

- Windows 7/8/10 taskbar feature
- Application-based menu
- Useful to:
 - open an app
 - a recently opened file
 - a recently opened folder
 - a recently opened website
- **Can contain much more references to opened files than “RecentDocs” and “Recent” folder**



Jumplists

- Stored in the User “Recent” folder
- **Two subfolders:**
 - AutomaticDestinations
 - CustomDestinations
- Every app as **unique AppID**
 - <https://github.com/EricZimmerman/JumpList/blob/master/JumpList/Resources/AppIDs.txt>
- **Creation time → First time of App Execution**
- **Modified time → Last time of App Execution**

```
Code Blame 732 lines (732 loc) · 33.8 KB
263 "7DCA40FD2A5A971F"|"LibreOffice 5.1.0.3"
264 "CD2ACD4089508507"|"AbsoluteTelnet 9.18 Lite"
265 "5F7B5F1E01B83767"|"Quick Access"
```

```
Code Blame 732 lines (732 loc) · 33.8 KB
614 6A316AA67A46820B | Core FTP LE 1.3C
615 "9F03AE476AD461FA"|"GroupsAloud 1.0"
616 "9D1F905CE5044AEE"|"Edge Browser"
```

```
Code Blame 732 lines (732 loc) · 33.8 KB
94 0500504000000000 | iTunes 9.0.0.70 / 9.2.1.5 /
95 "1C3057380FCF4155"|"Zenmap GUI 6.498ETA4"
96 "7E4DCA80246863E3"|"Control Panel - Settings"
97 "9027FE24326910D2"|"Thunderbird 38.6.0"
```

```
Code Blame 732 lines (732 loc) · 33.8 KB
316 "9149d0f5ebf7f710"|"Microsoft Outlook (15)"
317 "F01B4D95CF55D32A"|"Windows Explorer Windows 8.1"
318 F05000B7EE50FAC0 | MICROSOFT WORD 2010 64-bit
```

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	27/01/2017 00:14:26
5f7b5f1e01b83767.automaticDestinations...	2	Regular File	26/01/2017 23:44:47
7e4dca80246863e3.automaticDestination...	3	Regular File	27/01/2017 00:14:26
9d1f905ce5044aee.automaticDestinations...	4	Regular File	27/01/2017 00:28:00
f01b4d95cf55d32a.automaticDestinations...	8	Regular File	26/01/2017 23:44:33

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	27/01/2017 00:28:00
7e4dca80246863e3.customDestinations-ms	1	Regular File	26/01/2017 23:44:33
9d1f905ce5044aee.customDestinations-ms	1	Regular File	27/01/2017 00:28:00
f01b4d95cf55d32a.customDestinations-ms	1	Regular File	26/01/2017 23:44:33

Parsing a JumpList file

- **JLECmd** by Eric Zimmerman

```
C:\Windows\System32\cmd.exe

C:\ForensicTools\ZimmermanTools\net6>jlecmd
Description:
  JLECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/JLECmd

Examples: JLECmd.exe -f "C:\Temp\f01b4d95cf55d32a.customDestinations-ms" --mp
          JLECmd.exe -f "C:\Temp\f01b4d95cf55d32a.automaticDestinations-ms" --json "D:\jsonOutput" --jsonpretty
          JLECmd.exe -d "C:\CustomDestinations" --csv "c:\temp" --html "c:\temp" -q
          JLECmd.exe -d "C:\Users\e\AppData\Roaming\Microsoft\Windows\Recent" --dt "ddd yyyy MM dd HH:mm:ss.fff"

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Usage:
  JLECmd [options]

Options:
  -f <f>          File to process. Either this or -d is required
  -d <d>          Directory to recursively process. Either this or -f is required
  --all           Process all files in directory vs. only files matching *.automaticDestinations-ms or *.customDestinations-ms [default: False]
  --csv <csv>    Directory to save CSV formatted results to. This or --json required unless --de or --body is specified
  --csvf <csvf>  File name to save CSV formatted results to. When present, overrides default name
  --json <json>  Directory to save json representation to. Use --pretty for a more human readable layout
  --html <html>  Directory to save xhtml formatted results to. Be sure to include the full path in double quotes
  --pretty       When exporting to json, use a more human readable layout [default: False]
  -q            Only show the filename being processed vs all output. Useful to speed up exporting to json and/or csv [default: False]

  --ld           Include more information about lnk files [default: False]
  --fd           Include full information about lnk files (Alternatively, dump lnk files using --dumpTo and process with JLECmd) [default: False]
  --appIds <appIds> Path to file containing AppIDs and descriptions (appid|description format). New appIds are added to the built-in list, existing appIds will have their descriptions updated
  --dumpTo <dumpTo> Directory to save exported lnk files
  --dt <dt>      The custom date/time format to use when displaying timestamps. See https://goo.gl/CNVq0k for options. Default is: yyyy-MM-dd HH:mm:ss [default: yyyy-MM-dd HH:mm:ss]
  --mp          Display higher precision for timestamps [default: False]
  --withDir     When true, show contents of Directory not accounted for in DestList entries [default: False]
```

Parsing a single JumpList file

- **JLecmd.exe -f "AppID.automaticDestinations-ms"**

```
C:\ForensicTools\ZimmermanTools\net6>jlcmd -f "E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5d696d521de238c3.automaticDestinations-ms"
JLECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/JLECmd

Command line: -f E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5d696d521de238c3.automaticDestinations-ms

Warning: Administrator privileges not found!

Processing E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5d696d521de238c3.automaticDestinations-ms

Source file: E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5d696d521de238c3.automaticDestinations-ms

--- AppId information ---
AppID: 5d696d521de238c3
Description: Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116

--- DestList information ---
Expected DestList entries: 7
Actual DestList entries: 7
DestList version: 4

--- DestList entries ---
Entry #: 7
MRU: 0
Path: C:\Users\Sarah M\Desktop\what is this.html
Pinned: False
Created on: 1582-10-15 00:00:00
Last modified: 2017-02-02 22:52:25
Hostname:
Mac Address:
Interaction count: 1
```


Parsing a folder

- **JLecmd.exe -d <PATH-TO-FOLDER> --csv <PATH-TO-OUTPUT> -q**

```
Select C:\Windows\System32\cmd.exe
C:\ForensicTools\ZimmermanTools\net6>jlecmd -d "E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations" --csv D:\UNIGE\EXTRACTED\ -q
JLEcmd version 1.3.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/JLEcmd

Command line: -d E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations --csv D:\UNIGE\EXTRACTED\ -q
Warning: Administrator privileges not found!

Looking for jump list files in E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
Found 8 files

** JumpList has serialized property store(s)! View its contents via -f for details **

----- Processed E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\12dc1ea8e34b5a6.automaticDestinations-
ms in 0.06280960 seconds -----
** JumpList has serialized property store(s)! View its contents via -f for details **

----- Processed E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5d696d521de238c3.automaticDestinations
-ms in 0.00227980 seconds -----
** JumpList has serialized property store(s)! View its contents via -f for details **

----- Processed E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDestinations
-ms in 0.00264350 seconds -----
** JumpList has serialized property store(s)! View its contents via -f for details **

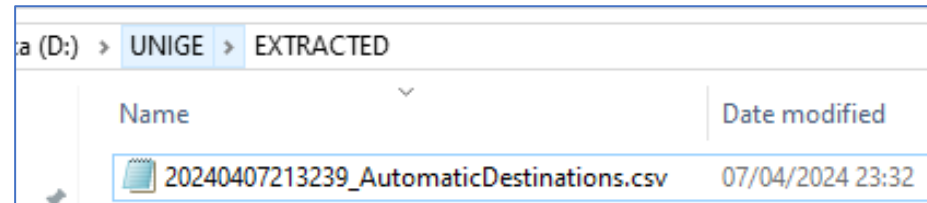
----- Processed E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9d1f905ce5044aee.automaticDestinations
-ms in 0.00181920 seconds -----
** JumpList has serialized property store(s)! View its contents via -f for details **

----- Processed E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\a52b0784bd667468.automaticDestinations
-ms in 0.00148970 seconds -----
** JumpList has serialized property store(s)! View its contents via -f for details **

----- Processed E:\Users\Sarah M\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\cb05cc8c5a282971.automaticDestinations
-ms in 0.00048930 seconds -----
** JumpList has serialized property store(s)! View its contents via -f for details **

UniGe 2025 - DFIR - Windows
```

Parsing a folder



20240407213239_AutomaticDestinations.csv

Drag a column header here to group by that column

Enter text to search...

Find

	Line	Tag	Sour...	Source Created	Source Modified	App Id	Pin Stat...	App Id Description	Last...	En...	M...	Creation T...	Last Modified	Path
Y	=			=	=				=		=	=	=	
1		<input type="checkbox"/>	E:\U...	2017-01-27 17:21:49	2017-01-27 17:21:49	12dc1ea8e34b5a6	False	Microsoft Paint 6...	1	1	0	2017-01-27...	2017-01-27 17:21:49	C:\Users\Sarah M\Desktop\pets\Great Horned Owl.jpg
2		<input type="checkbox"/>	E:\U...	2017-01-27 01:16:48	2017-02-02 22:52:25	5d696d521de238c3	False	Google Chrome 9.0...	7	7	0		2017-02-02 22:52:25	C:\Users\Sarah M\Desktop\what is this.html
3		<input type="checkbox"/>	E:\U...	2017-01-27 01:16:48	2017-02-02 22:52:25	5d696d521de238c3	False	Google Chrome 9.0...	7	6	1		2017-02-02 22:51:41	C:\Users\Sarah M\Desktop\WOLF Awesome.html
4		<input type="checkbox"/>	E:\U...	2017-01-27 01:16:48	2017-02-02 22:52:25	5d696d521de238c3	False	Google Chrome 9.0...	7	5	2		2017-01-31 19:15:03	C:\Users\Sarah M\Desktop\Snowy Owl.pdf
5		<input type="checkbox"/>	E:\U...	2017-01-27 01:16:48	2017-02-02 22:52:25	5d696d521de238c3	False	Google Chrome 9.0...	7	4	3	2017-01-30...	2017-01-31 19:10:30	C:\Users\Sarah M\Documents\New Pet Care\Owl_Emergency...
6		<input type="checkbox"/>	E:\U...	2017-01-27 01:16:48	2017-02-02 22:52:25	5d696d521de238c3	False	Google Chrome 9.0...	7	3	4		2017-01-31 19:09:10	C:\Users\Sarah M\Downloads\Owl_Keeping.pdf
7		<input type="checkbox"/>	E:\U...	2017-01-27 01:16:48	2017-02-02 22:52:25	5d696d521de238c3	False	Google Chrome 9.0...	7	2	5		2017-01-31 19:08:59	C:\Users\Sarah M\Downloads\Owl_Emergency_Care.pdf
8		<input type="checkbox"/>	E:\U...	2017-01-27 01:16:48	2017-02-02 22:52:25	5d696d521de238c3	False	Google Chrome 9.0...	7	1	6		2017-01-27 01:16:48	C:\Users\Sarah M\Downloads\Great Horned Owl Info.pdf
9		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	13	0		2017-02-02 22:52:25	C:\Users\Sarah M\Desktop\what is this.html
10		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	12	1		2017-02-02 22:51:41	C:\Users\Sarah M\Desktop\WOLF Awesome.html
11		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	A	2	2017-01-30...	2017-02-02 22:39:08	C:\Users\Sarah M\Documents\New Pet Care\Owl_Emergency...
12		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	11	3		2017-02-02 22:38:39	F:\Snowy Owl.pdf
13		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	10	4		2017-02-02 22:38:35	F:\Snowy Owl Care.pdf
14		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	E	5		2017-02-02 22:38:25	F:\My New Pet.jpg
15		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	F	6	2017-01-30...	2017-02-02 22:00:42	C:\Users\Sarah M\Documents\New Pet Care\My New Pet.jp
16		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	D	7		2017-01-31 19:27:24	C:\Users\Sarah M\Desktop\Next pet
17		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	C	8		2017-01-31 19:15:03	C:\Users\Sarah M\Documents\New Pet Care\Snowy Owl.pdf
18		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	9	9		2017-01-31 19:09:10	C:\Users\Sarah M\Downloads\Owl_Keeping.pdf
19		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	8	10		2017-01-31 19:08:59	C:\Users\Sarah M\Downloads\Owl_Emergency_Care.pdf
20		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	7	11		2017-01-28 22:36:41	C:\Users\Sarah M\Downloads\Background.jpg
21		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	6	12		2017-01-28 22:34:42	C:\Users\Sarah M\Downloads\Cool picture of a tiger ma
22		<input type="checkbox"/>	E:\U...	2017-01-27 00:53:54	2017-02-02 22:52:25	5f7b5f1e01b83767	False	Quick Access	19	4	13	2017-01-27...	2017-01-27 17:23:25	C:\Users\Sarah M\Desktop\pets\Snowy Owl.jpg
23		<input type="checkbox"/>	E:\U...	2017-01-27 17:22:22	2017-02-02 22:39:08	9d1f905ce5044aee	False	Edge Browser	5	3	0	2017-01-30...	2017-02-02 22:39:08	C:\Users\Sarah M\Documents\New Pet Care\Owl_Emergency...
24		<input type="checkbox"/>	E:\U...	2017-01-27 17:22:22	2017-02-02 22:39:08	9d1f905ce5044aee	False	Edge Browser	5	5	1		2017-02-02 22:38:39	F:\Snowy Owl.pdf
25		<input type="checkbox"/>	E:\U...	2017-01-27 17:22:22	2017-02-02 22:39:08	9d1f905ce5044aee	False	Edge Browser	5	4	2		2017-02-02 22:38:35	F:\Snowy Owl Care.pdf
26		<input type="checkbox"/>	E:\U...	2017-01-27 17:22:22	2017-02-02 22:39:08	9d1f905ce5044aee	False	Edge Browser	5	2	3		2017-01-30 22:45:44	http://go.microsoft.com/fwlink/?LinkID=219472&clcid=0
27		<input type="checkbox"/>	E:\U...	2017-01-27 17:22:22	2017-02-02 22:39:08	9d1f905ce5044aee	False	Edge Browser	5	1	4		2017-01-27 17:22:22	microsoft-edge:https://www.bing.com/search?q=view+rib
28		<input type="checkbox"/>	E:\U...	2017-01-27 17:23:03	2017-02-02 22:38:25	a52b0784bd667468	False	Photos Microsoft ...	5	5	0		2017-02-02 22:38:25	F:\My New Pet.jpg
29		<input type="checkbox"/>	E:\U...	2017-01-27 17:23:03	2017-02-02 22:38:25	a52b0784bd667468	False	Photos Microsoft ...	5	4	1	2017-01-30...	2017-02-02 22:00:42	C:\Users\Sarah M\Documents\New Pet Care\My New Pet.jp
30		<input type="checkbox"/>	E:\U...	2017-01-27 17:23:03	2017-02-02 22:38:25	a52b0784bd667468	False	Photos Microsoft ...	5	3	2	2017-01-27...	2017-01-27 17:23:29	C:\Users\Sarah M\Desktop\pets\Pygmy Owl.jpg
31		<input type="checkbox"/>	E:\U...	2017-01-27 17:23:03	2017-02-02 22:38:25	a52b0784bd667468	False	Photos Microsoft ...	5	2	3	2017-01-27...	2017-01-27 17:23:25	C:\Users\Sarah M\Desktop\pets\Snowy Owl.jpg
32		<input type="checkbox"/>	E:\U...	2017-01-27 17:23:03	2017-02-02 22:38:25	a52b0784bd667468	False	Photos Microsoft ...	5	1	4	2017-01-27...	2017-01-27 17:23:03	C:\Users\Sarah M\Desktop\pets\Great Horned Owl.jpg
33		<input type="checkbox"/>	E:\U...	2017-01-27 00:35:15	2017-02-02 22:52:25	f01b4d95cf55d32a	True	Windows Explorer ...	8	1	0	2017-01-26...	2017-02-02 22:52:25	knownfolder:{754AC886-DF64-4CBA-86B5-F7FBF4FBCFE5} ==

Exercise 8

1. Which application has the AppID **5d696d521de238c3**?
2. How many files were opened with the app with AppID **5d696d521de238c3** by the **Sarah M** user?
3. Based on the analysis of JumpList files, which **keyword was searched by the Sarah M user on Bing**? Which **browser was used** for these searches?
4. Which files were opened with the **Microsoft Photos** app?

Exercise 8.1 / 8.2 / 8.3 / 8.4

5d696d521de238c3	False	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116	7	7	0		2017-02-02 22:52:25	C:\Users\Sarah M\Desktop\what is this.html
5d696d521de238c3	False	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116	7	6	1		2017-02-02 22:51:41	C:\Users\Sarah M\Desktop\WOLF Awsome.html
5d696d521de238c3	False	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116	7	5	2		2017-01-31 19:15:03	C:\Users\Sarah M\Desktop\Snowy_Owl.pdf
5d696d521de238c3	False	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116	7	4	3	2017-01-30...	2017-01-31 19:10:30	C:\Users\Sarah M\Documents\New Pet Care\Owl_Emergency_Care.pdf
5d696d521de238c3	False	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116	7	3	4		2017-01-31 19:09:10	C:\Users\Sarah M\Downloads\Owl_Keeping.pdf
5d696d521de238c3	False	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116	7	2	5		2017-01-31 19:08:59	C:\Users\Sarah M\Downloads\Owl_Emergency_Care.pdf
5d696d521de238c3	False	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 48.0.2564.116	7	1	6		2017-01-27 01:16:48	C:\Users\Sarah M\Downloads\Great Horned Owl Info.pdf

9d1f905ce5044aee	False	Edge Browser	5	2	3		2017-01-30 22:45:44	http://go.microsoft.com/fwlink/?LinkID=219472&clid=0x409
9d1f905ce5044aee	False	Edge Browser	5	1	4		2017-01-27 17:22:22	microsoft-edge:https://www.bing.com/search?q=view+ribbon&form=

a52b0784bd667468	False	Photos Microsoft 16.526.11220.0 (Windows 10)	5	5	0		2017-02-02 22:38:25	F:\My New Pet.jpg
a52b0784bd667468	False	Photos Microsoft 16.526.11220.0 (Windows 10)	5	4	1	2017-01-30...	2017-02-02 22:00:42	C:\Users\Sarah M\Documents\New Pet Care\My New Pet.jpg
a52b0784bd667468	False	Photos Microsoft 16.526.11220.0 (Windows 10)	5	3	2	2017-01-27...	2017-01-27 17:23:29	C:\Users\Sarah M\Desktop\pets\Pygmy Owl.jpg
a52b0784bd667468	False	Photos Microsoft 16.526.11220.0 (Windows 10)	5	2	3	2017-01-27...	2017-01-27 17:23:25	C:\Users\Sarah M\Desktop\pets\Snowy Owl.jpg
a52b0784bd667468	False	Photos Microsoft 16.526.11220.0 (Windows 10)	5	1	4	2017-01-27...	2017-01-27 17:23:03	C:\Users\Sarah M\Desktop\pets\Great Horned Owl.jpg