OS Forensics Final Case

FOR340

Investigation Conducted By: Noah Beckman & Dylan Navarro

April 2022

Table of Contents

Objectives

This investigation is being conducted to examine alerts the network monitoring system has set off. The alerts point to a few machines on the network containing suspicious activity. The investigators have been tasked with reviewing the images provided and determining if an attack occurred. In addition, it is suspected that the domain administrator credentials have been compromised and data exfiltration of confidential information occurred. Our objective is to figure out what happened and what the attacker might have done.

The network monitoring system reported the following:

- A connection from one workstation to the other for file sharing purposes.
- A remote login to both of these workstations.
- Outgoing connections that we believe are part of some data exfiltration.

Tools

- FTK Imager
- Registry Explorer
- LECmd
- Timeline Explorer
- JumpListExplorer
- PECmd
- EvtxECmd
- WinPrefetchview
- ShellBagsExplorer
- ThumbCacheViewer
- Dcode
- Kali Linux
- Hashcat
- Axiom

Notation Information

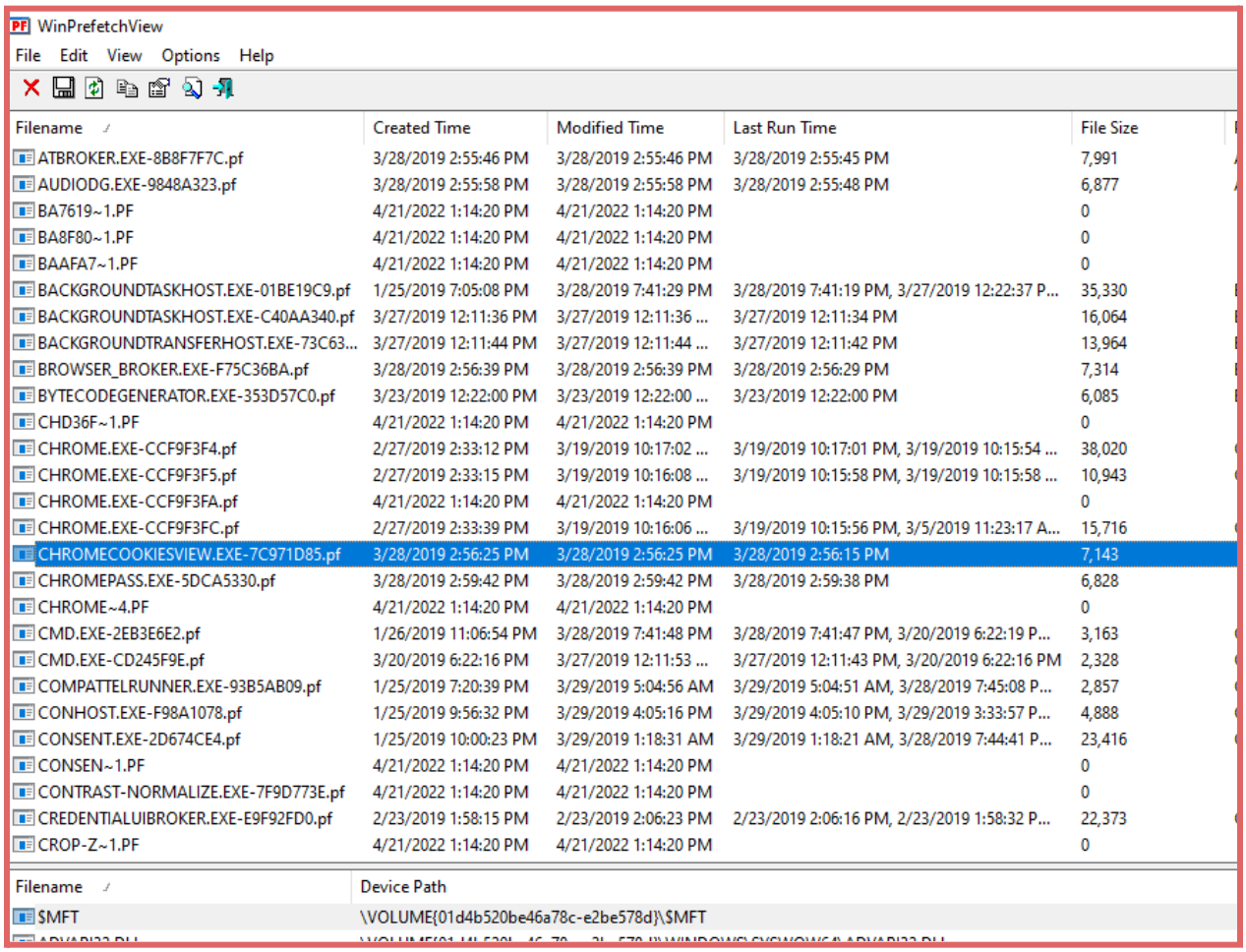
Within this report various screenshots will be notated with captions and a surrounding colored box. The color of the box represents which computer was being shown in the screenshot. For the purpose of this report light red border represents It-wks01 and purple represents prog-wks03.

Methodology

During this investigation, I found various forensically relevant artifacts related to the reported alerts from the network monitoring system. Using a variety of forensic tools, I was able to extract key artifacts

showing the underlying issues as to what happened on these two systems. The following subsections will explain what each artifact is, where it was found, and how the tool is used to parse the artifact information. Later on, under the investigation findings page I will discuss how the found artifacts from these locations and tools relate to the investigation.

Prefetch

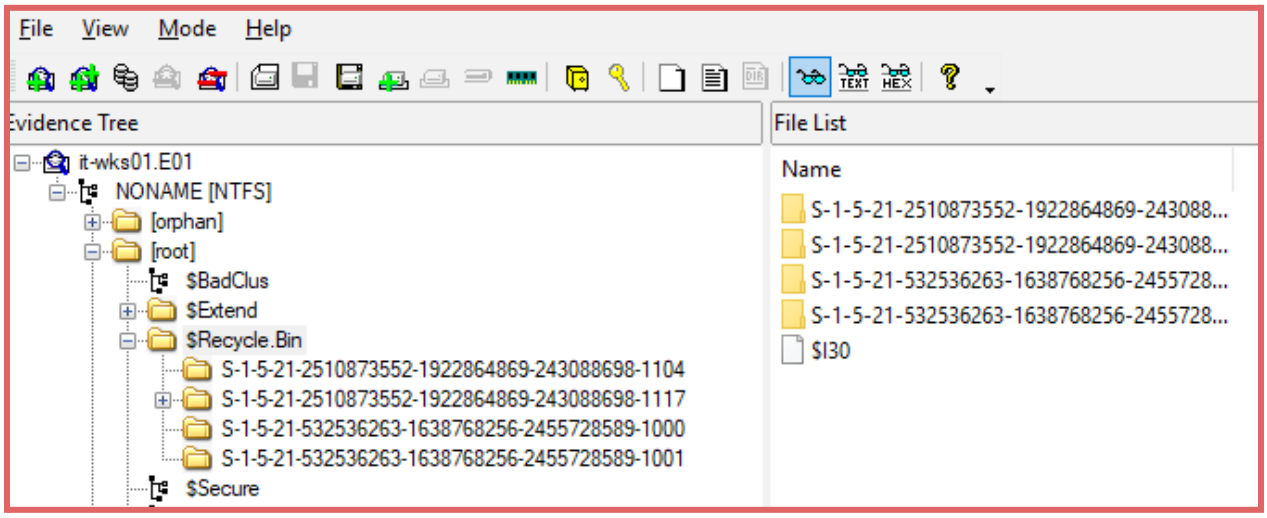


Filename	Created Time	Modified Time	Last Run Time	File Size
ATBROKER.EXE-8B8F7F7C.pf	3/28/2019 2:55:46 PM	3/28/2019 2:55:46 PM	3/28/2019 2:55:45 PM	7,991
AUDIODG.EXE-9848A323.pf	3/28/2019 2:55:58 PM	3/28/2019 2:55:58 PM	3/28/2019 2:55:48 PM	6,877
BA7619~1.PF	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0
BA8F80~1.PF	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0
BAAFA7~1.PF	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0
BACKGROUNDTASKHOST.EXE-01BE19C9.pf	1/25/2019 7:05:08 PM	3/28/2019 7:41:29 PM	3/28/2019 7:41:19 PM, 3/27/2019 12:22:37 P...	35,330
BACKGROUNDTASKHOST.EXE-C40AA340.pf	3/27/2019 12:11:36 PM	3/27/2019 12:11:36 ...	3/27/2019 12:11:34 PM	16,064
BACKGROUNDTRANSFERHOST.EXE-73C63...	3/27/2019 12:11:44 PM	3/27/2019 12:11:44 ...	3/27/2019 12:11:42 PM	13,964
BROWSER_BROKER.EXE-F75C36BA.pf	3/28/2019 2:56:39 PM	3/28/2019 2:56:39 PM	3/28/2019 2:56:29 PM	7,314
BYTECODEGENERATOR.EXE-353D57C0.pf	3/23/2019 12:22:00 PM	3/23/2019 12:22:00 ...	3/23/2019 12:22:00 PM	6,085
CHD36F~1.PF	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0
CHROME.EXE-CCF9F3F4.pf	2/27/2019 2:33:12 PM	3/19/2019 10:17:02 ...	3/19/2019 10:17:01 PM, 3/19/2019 10:15:54 ...	38,020
CHROME.EXE-CCF9F3F5.pf	2/27/2019 2:33:15 PM	3/19/2019 10:16:08 ...	3/19/2019 10:15:58 PM, 3/19/2019 10:15:58 ...	10,943
CHROME.EXE-CCF9F3FA.pf	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0
CHROME.EXE-CCF9F3FC.pf	2/27/2019 2:33:39 PM	3/19/2019 10:16:06 ...	3/19/2019 10:15:56 PM, 3/5/2019 11:23:17 A...	15,716
CHROMECOOKIESVIEW.EXE-7C971D85.pf	3/28/2019 2:56:25 PM	3/28/2019 2:56:25 PM	3/28/2019 2:56:15 PM	7,143
CHROMEPASS.EXE-5DCA5330.pf	3/28/2019 2:59:42 PM	3/28/2019 2:59:42 PM	3/28/2019 2:59:38 PM	6,828
CHROME~4.PF	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0
CMD.EXE-2EB3E6E2.pf	1/26/2019 11:06:54 PM	3/28/2019 7:41:48 PM	3/28/2019 7:41:47 PM, 3/20/2019 6:22:19 P...	3,163
CMD.EXE-CD245F9E.pf	3/20/2019 6:22:16 PM	3/27/2019 12:11:53 ...	3/27/2019 12:11:43 PM, 3/20/2019 6:22:16 PM	2,328
COMPATTELRUNNER.EXE-93B5AB09.pf	1/25/2019 7:20:39 PM	3/29/2019 5:04:56 AM	3/29/2019 5:04:51 AM, 3/28/2019 7:45:08 P...	2,857
CONHOST.EXE-F98A1078.pf	1/25/2019 9:56:32 PM	3/29/2019 4:05:16 PM	3/29/2019 4:05:10 PM, 3/29/2019 3:33:57 P...	4,888
CONSENT.EXE-2D674CE4.pf	1/25/2019 10:00:23 PM	3/29/2019 1:18:31 AM	3/29/2019 1:18:21 AM, 3/28/2019 7:44:41 P...	23,416
CONSEN~1.PF	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0
CONTRAST-NORMALIZE.EXE-7F9D773E.pf	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0
CREDENTIALUIBROKER.EXE-E9F92FD0.pf	2/23/2019 1:58:15 PM	2/23/2019 2:06:23 PM	2/23/2019 2:06:16 PM, 2/23/2019 1:58:32 P...	22,373
CROP-Z~1.PF	4/21/2022 1:14:20 PM	4/21/2022 1:14:20 PM		0

Filename	Device Path
$MFT	\VOLUME{01d4b520be46a78c-e2be578d}\$MFT

In order to analyze prefetch files I used the program WinPrefetchView. This application allows an investigator to view the prefetch files within a specific folder. The files for prefetch can be found under `C:\Windows\Prefetch`. Prefetch files are used by Windows as a way to optimize boot and program startup. Each prefetch file has a .pf extension and gets created whenever a program is executed. A new prefetch file is created whenever a program is executed from a different location.

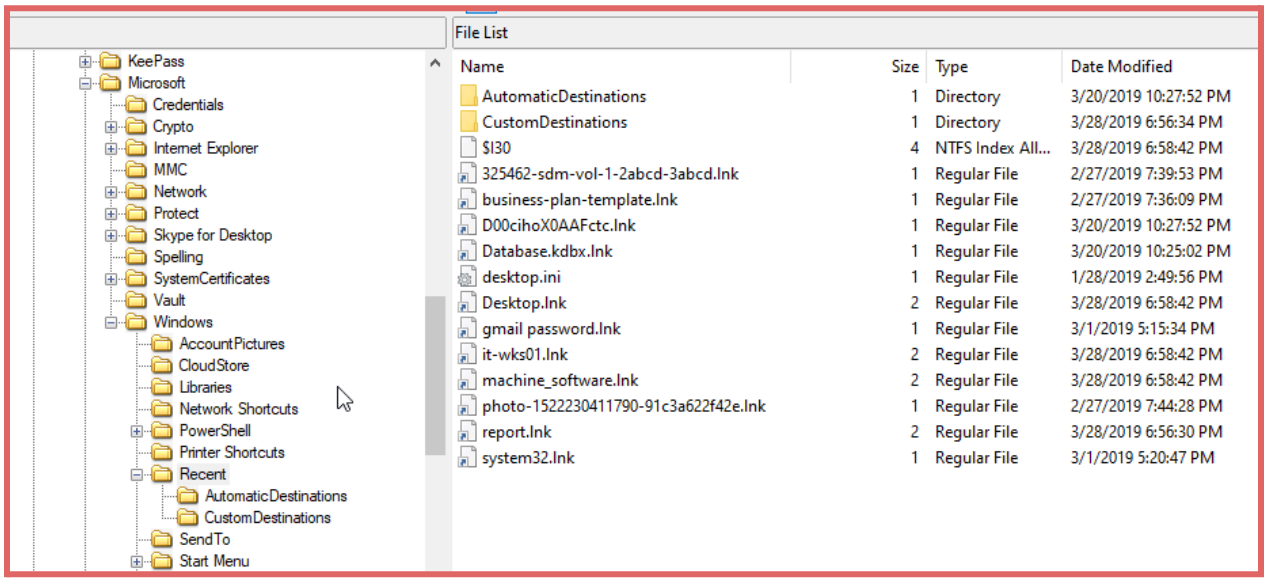
Recycle Bin



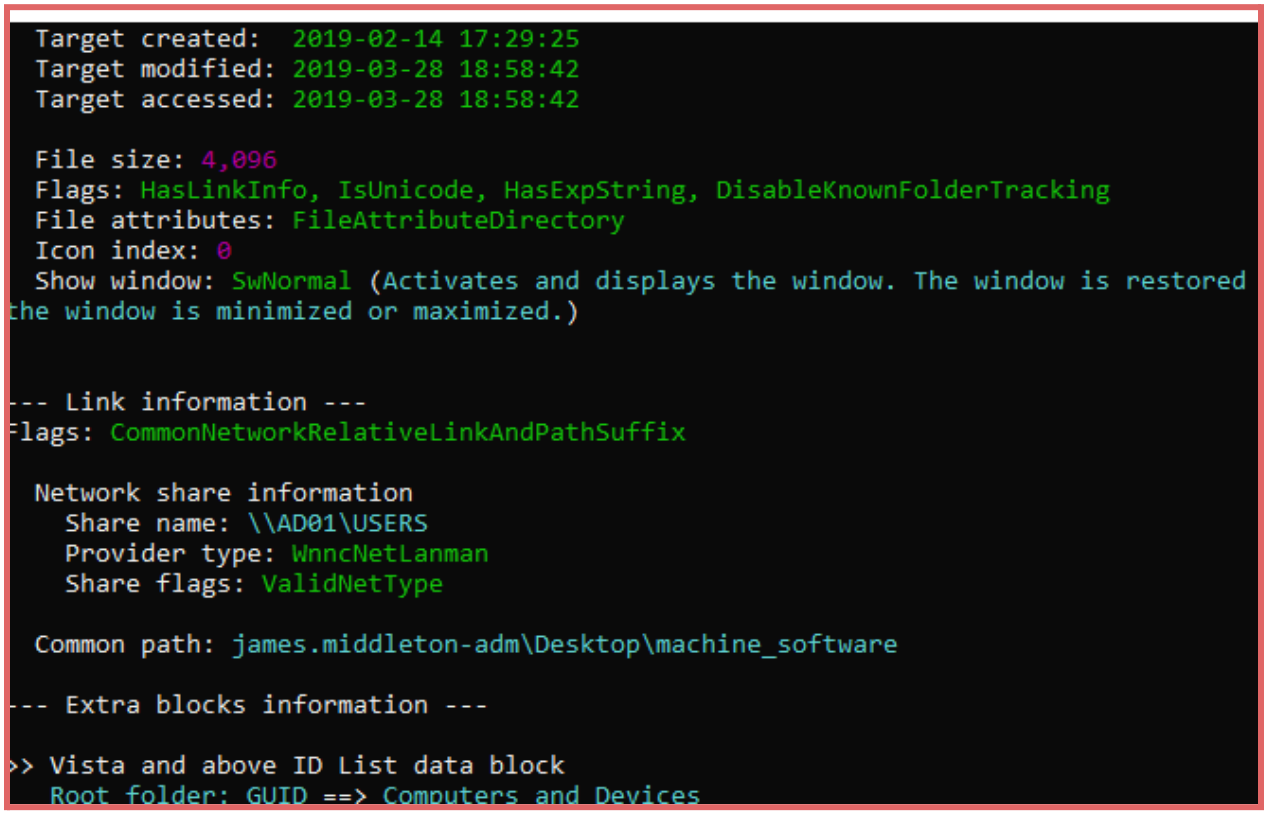
The recycle bin is a great way to see if a user attempted to delete files and forgot to empty the recycle bin. Looking at this directory also shows the user SIDs. This is forensically relevant as information about the user can be connected back to this directory. This directory can be found using FTK imager under `C:\$Recycle.Bin`. FTK imager is a form of data preview and imaging tool. All of the evidence in this case was extracted using FTK imager.

Lnk Files

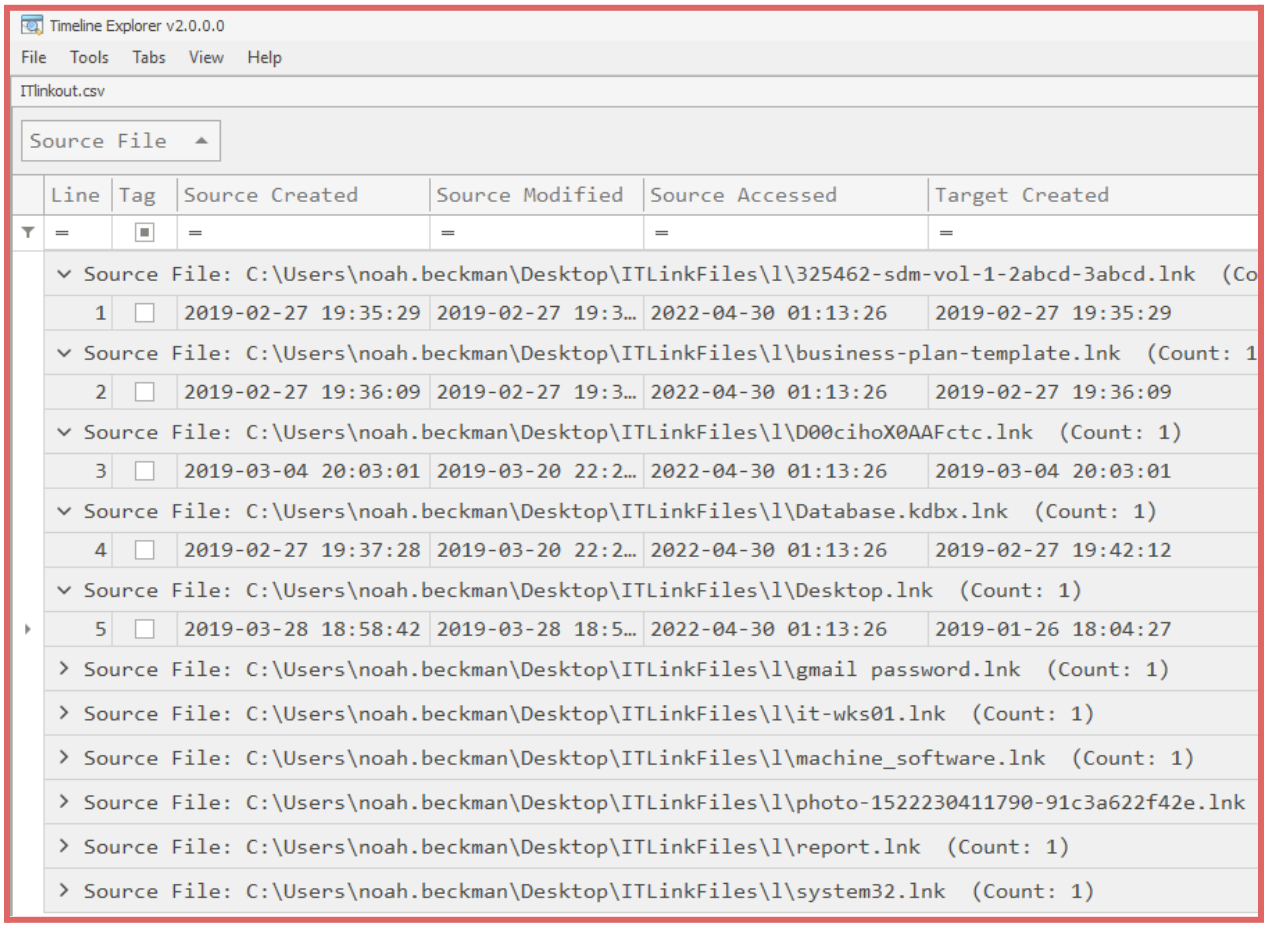
A lnk file is a type of file that contains a target identifier and some other metadata information. The important part is that it is essentially a shortcut. This is forensically relevant to the investigation because when a malicious user is exploiting a system they will often delete files from the system. While the deleted files are what we are looking for, lnk files are created whenever the application is run and are not deleted with the file. This means we can extract the vital information about the specific file by analyzing the lnk. Important information found in lnk files include timestamps, full path location, and volume serial number of the partition.



The abovescreenshot shows where lnk files are located on a system and where they were extracted from. Lnk files are stored under `C:\Users\<Username>\AppData\Roaming\Microsoft\Windows\Recent`
Exporting the files using FTK imager allows for the investigator to use additional tools in the future to further investigate the device.

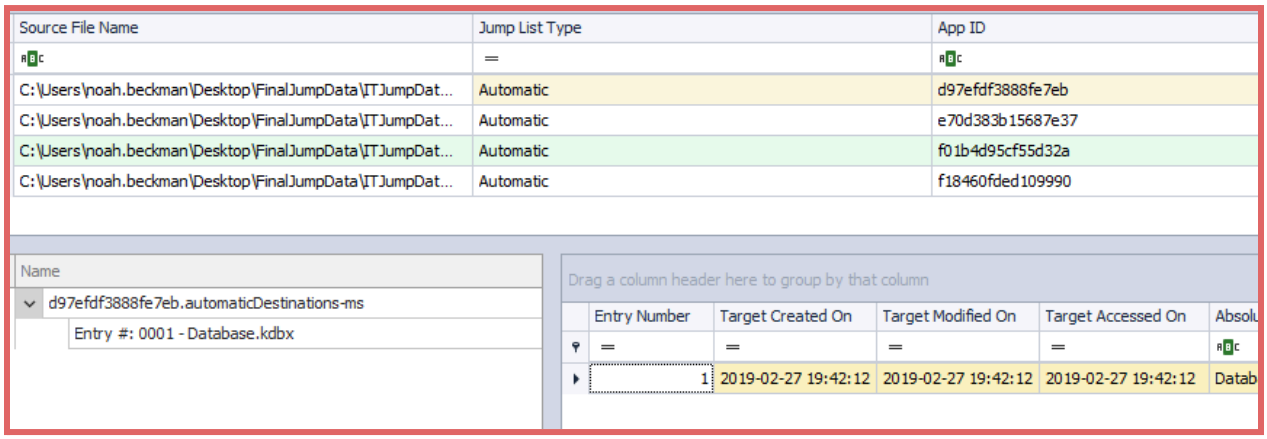


One such tool is LECmd. This tool is a lnk file parser. The command I ran in Command Prompt to parse the file is: `LECmd.exe -d "C:\Users\noah.beckman\Desktop\ITLinkFiles\l" --csv ITLinkout.` This command exports the results to a csv document. Analyzing data in a csv makes reading the results more clear.



Another helpful tool that helps visualize csv data is Timeline Explorer. This program allows you to view a CSV and apply filters to the data to sort by specific columns. For example, in the screenshot above I sorted all the lnk files by their source file location. This allows you to expand the entry and see all the relevant information for that file.

Jump Lists

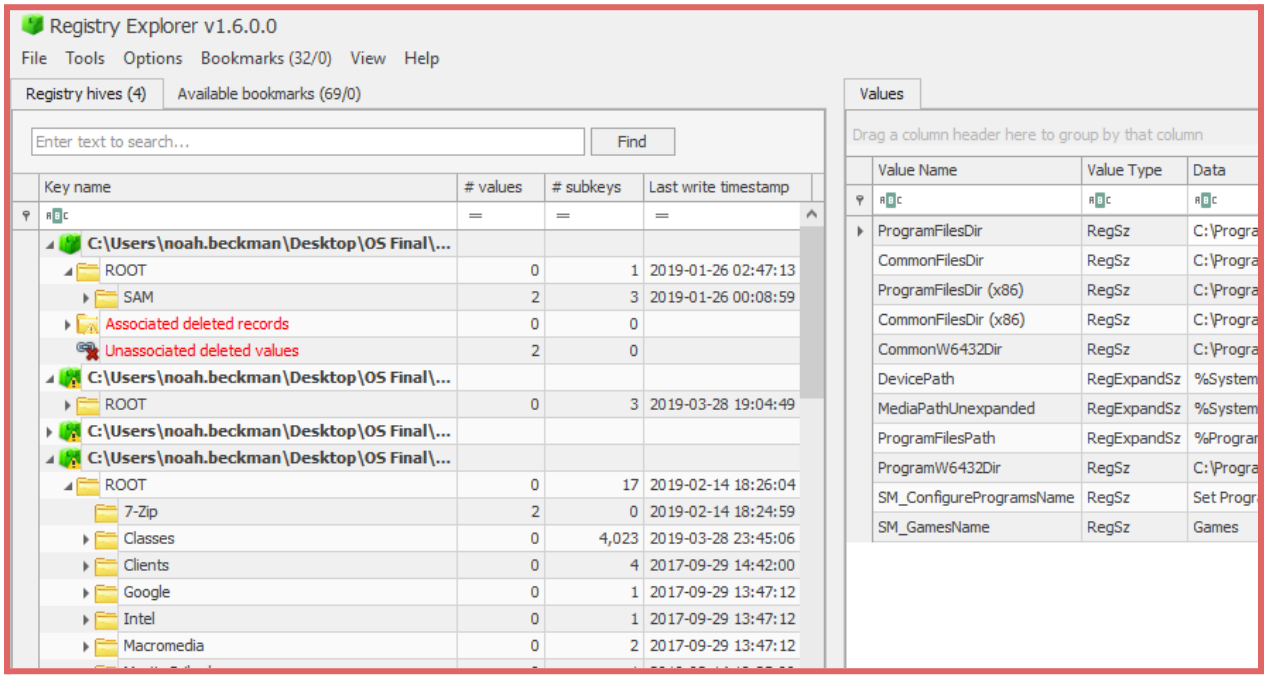


Jump lists are another important artifact to look at. They are files containing most recently used or frequently used documents compiled into one. They differ from previous artifacts because they are not based on .lnk files or registry. Like before, these artifacts remain even when an application or document

has been deleted. They can be found under `C:\Users\[Profile]\AppData\Roaming\Microsoft\Windows\Recent\`. The jump list files are found in two folders Automatic and Custom. They have to be extracted with FTK imager. The screenshot above shows the tool JumpListExplorer. Within this tool you can view all the important metadata related to the jump list files.

Windows Registry

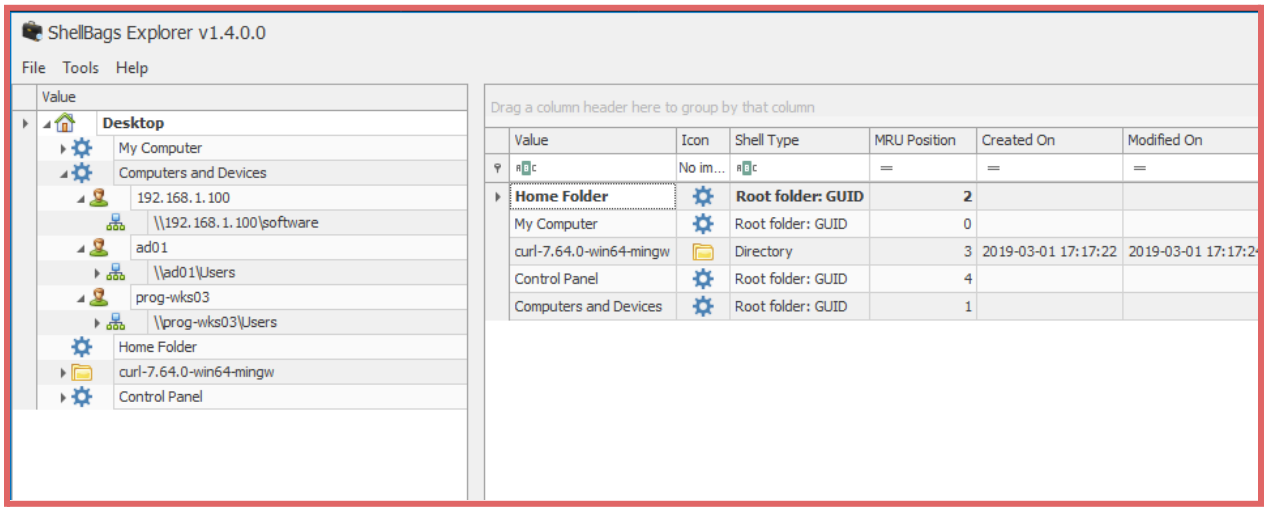
Windows registry is an important feature of Windows. It contains a large amount of relevant information regarding what is happening on the system. The registry is a hierarchical database that is used to configure the OS and most programs. The information here is forensically relevant as most of any user on the machine's history is tracked here. This includes usernames, history of websites, recently opened files, and more.



This screenshot shows the tool Registry Explorer. This tool allows an investigator to explore the different registry hives that registry information is stored in. The program also parses the data into a readable format. Most of the device information regarding the systems of this case will come from the registry. The registry files can be found in a couple locations depending on the artifact you are looking for, but most of them are located: `C:\Windows\System32\config`. Additional user specifc registry files are located in `C:\Users\[Profile]`.

Shell Bags

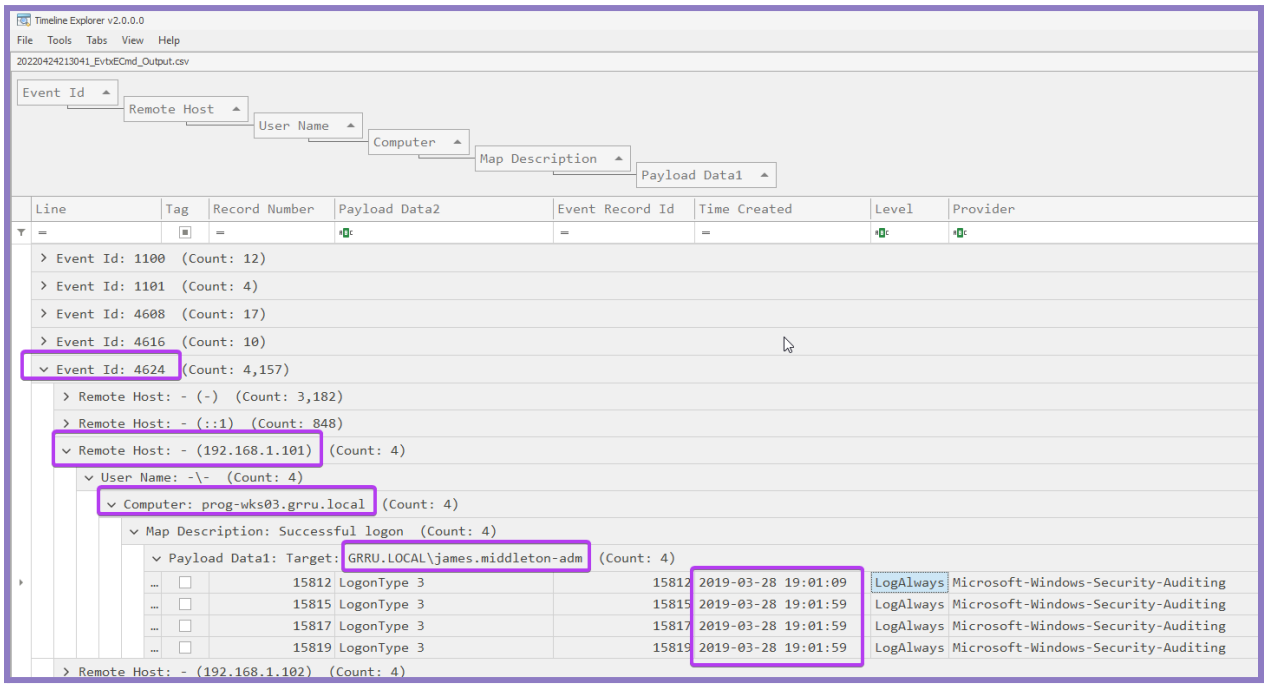
Shell bags are a type of artifact that are created when a folder or application is interacted with or its settings are changed. This is important as it allows the investigator to continue to create a timeline of events that the user interacted with.



This screenshot shows the tool Shellbags Explorer. This application allows an investigator to visualize the shellbag artifacts from a target system. These logs can be found in a file called USRCLASS.DAT. This file is located at: `USERPROFILE\AppData\Local\Microsoft\Windows.` Once the whole drive is exported from FTK imager, you can access this file directly.

Windows Event Logs

Windows event logs are a great way to plot out what a user was doing. Like the name suggests, this artifact is a collection of logs that Windows makes given on certain actions. These are forensically relevant as an investigator can use the log information to determine if connections were made, malware was detected, and much more.

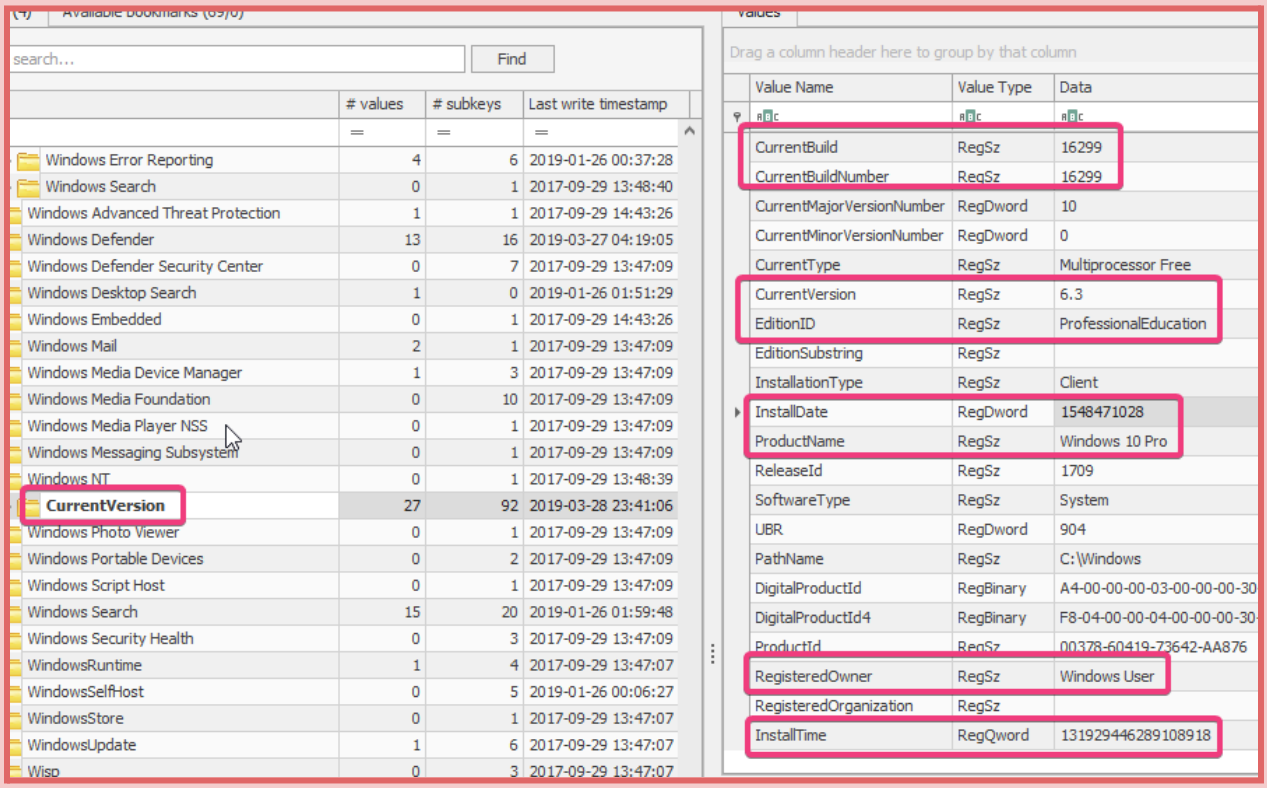


This screenshot shows Timeline Explorer again. However, to acquire the csv data a the tool ExtxECmd was used to turn the event log data to a csv. Timeline explorer works really well with logs like this because you can sort by event id and other column information to tailor your filter for what you are looking for. The event log files can be found at: `[root]\Windows\System32\winevt\Logs.`

Acquisition Information

lt-wks01

MD5 Hash: 287772ce6da275a146e1765a9a2f1ea4
SHA1 Hash: ae576547f34c9a80dbdca1345901ed9a2e2e5a53
Acquire Date: 3/29/2019 8:12:31 PM
Disk Volume Size: 40.8 GB
Volume Serial Number: E2BE-578D



System information from registry - `SOFTWARE/Microsoft/Windows NT/CurrentVersion`

Product: Windows 10 Pro
Edition: Professional Education
Release ID: 1709
Build Number: 16299
Registered User: Windows User

Value Name	Value Data
Bias	300
DaylightBias	-60
DaylightName	@tzres.dll,-111
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
StandardBias	0
StandardName	@tzres.dll,-112
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
TimeZoneKeyName	Eastern Standard Time
ActiveTimeBias	240

IT-Wks01 Timezone information -
`SYSTEM/ControlSet001/Control/TimeZoneInformation`

Looking at the TimeZoneKeyName in the above image we can see the system is set to use the Eastern Standard Time timezone. We can see that the bias for that timezone is 300. We can also see that the ActiveTimeBias value is currently set to 240. This indicates that the DaylightBias value is being applied meaning at the time of image acquistion the system was observing daylight savings.

Value Name	Value Type	Data
EnableDHCP	RegDword	1
Domain	RegSz	
NameServer	RegSz	
DhcpIPAddress	RegSz	192.168.1.101
DhcpSubnetMask	RegSz	255.255.255.0
DhcpServer	RegSz	192.168.1.253
Lease	RegDword	691200
LeaseObtainedTime	RegDword	39
T1	RegDword	345639
T2	RegDword	604839
LeaseTerminatesTime	RegDword	691239
AddressType	RegDword	0
IsServerNapAware	RegDword	0
DhcpConnForceBroadcastFlag	RegDword	0
DhcpInterfaceOptions	RegBinary	0F-00-00-00-00-00-00-00-0B-00-00-00-00-00-00-00-27-8C
DhcpDomain	RegSz	grru.local
DhcpNameServer	RegSz	192.168.1.254
DhcpDefaultGateway	RegMultiSz	192.168.1.1
DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0
DhcpGatewayHardware	RegBinary	C0-A8-01-01-06-00-00-00-00-0C-29-CF-28-9B
DhcpGatewayHardwareCount	RegDword	1

IT-wks01 Network information -
SYSTEM/ControlSet001/Services/Tcpip/Parameters/Interfaces/{d338b54a-5437-499b-b434-e6372a614f8c}
Last IP: 192.168.1.101/24
DNS Server: 192.168.1.254
Gateway: 192.168.1.1
DHCP Server: 192.168.1.253
DHCP Domain: grru.local

User Name	User...	Last Login Time	Total Login ...	Created On	Valid U
Administrator	500		0	2019-01-26 02:50:28	☑
Guest	501		0	2019-01-26 02:50:28	☑
DefaultAccount	503		0	2019-01-26 02:50:28	☑
WDAGUtilityAccount	504		0	2019-01-26 02:50:28	☑
Admin	1001	2019-01-28 14:48:23	8	2019-01-26 02:54:18	☑

IT-wks01 accounts - `SAM\Domains\Account\Users`

Drag a column header here to group by that column

Timestamp	Key Name	Profile Image Path
2017-09-29 13:48:39	S-1-5-18	%systemroot%\system32\config\systemprofile
2019-01-26 02:47:16	S-1-5-19	C:\Windows\ServiceProfiles\LocalService
2019-01-26 02:47:14	S-1-5-20	C:\Windows\ServiceProfiles\NetworkService
2019-01-27 03:33:49	S-1-5-21-2510873552-1922864869-243088698-1104	C:\Users\james.middleton
2019-02-13 23:45:03	S-1-5-21-2510873552-1922864869-243088698-1117	C:\Users\james.middleton-adm
2019-01-27 03:51:11	S-1-5-21-532536263-1638768256-2455728589-1001	C:\Users\Admin

More user information including domain accounts - `SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`

For additional information on local user accounts see Appendix 4

Image USB Information

There is one USB that was used on IT-wks01 and no USB connections on Prog-wks03. This information was collected through a variety of registry keys. Paths to each key are below.

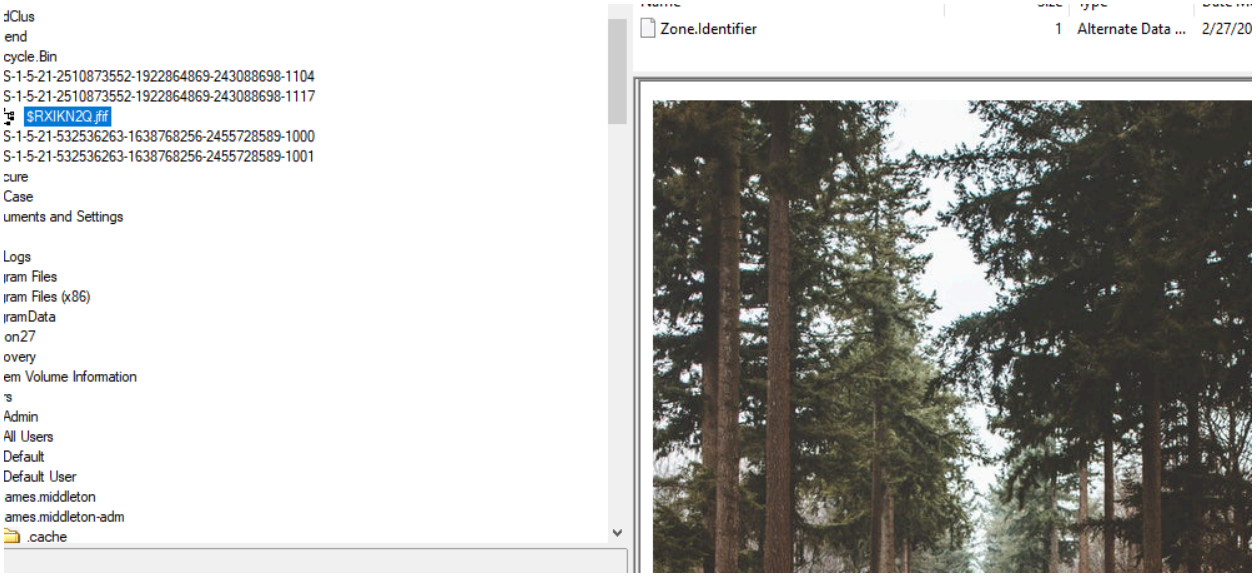
- `SYSTEM\ControlSet001\Enum\USBSTOR`
- `SYSTEM\ControlSet001\Enum\USB`
- `SYSTEM\MountedDevices`
- `SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt`

Product Name: Prod_Trancend_64
Vendor Name: JetFlash
Version: 1100

Product ID: 1000
Vendor ID: 8564
Serial Number: 05OWFMARTD8LUHG6&0
Unique Instance ID: 3456799116
GUID: 53f56307-b6bf-11d0-94f2-00a0c91efb8b
Volume Label: Sloth
Drive Letter: E:
First Installed: 2019-02-14 18:21:55
Last Connected: 2019-02-14 18:21:55
Last Removed: 2019-02-14 18:42:02

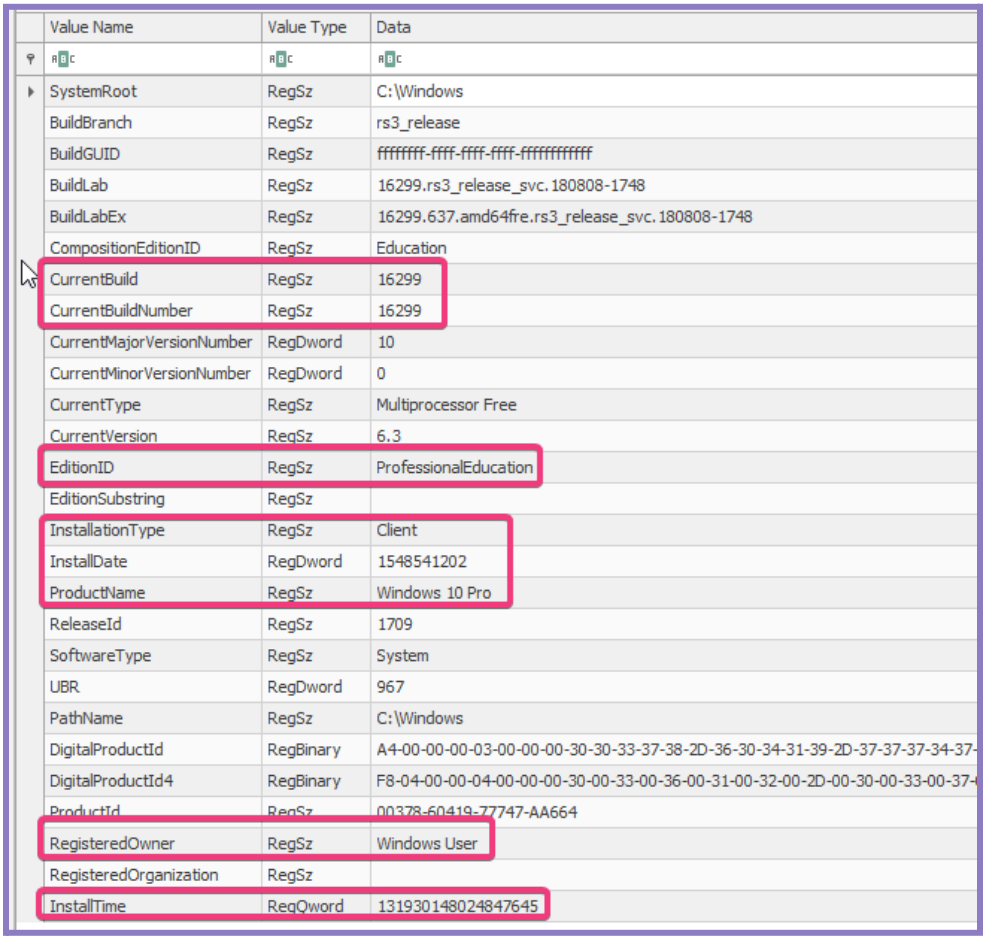
Deleted Files

After examining the $Recycle bin folder using FTK imager, it was found that one photo was deleted by user James.middleton-adm. We can tell this is the user by comparing the keyname value from the Profile List screenshot above and comparing it to the identifier in the recycle bin.



Prog-wks03

MD5 Hash: e0ec4d5aa7d073d03fce399fda4277fa
SHA1 Hash: ab646bc506457ba80fafd3c8fee7b7203492639a
Acquire Date: 3/30/2019 10:58:21 PM
Disk Volume Size: 24984 MB
Volume Serial Number: 8CB6-8B7D



Value Name	Value Type	Data
SystemRoot	RegSz	C:\Windows
BuildBranch	RegSz	rs3_release
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	RegSz	16299.rs3_release_svc.180808-1748
BuildLabEx	RegSz	16299.637.amd64fre.rs3_release_svc.180808-1748
CompositionEditionID	RegSz	Education
CurrentBuild	RegSz	16299
CurrentBuildNumber	RegSz	16299
CurrentMajorVersionNumber	RegDword	10
CurrentMinorVersionNumber	RegDword	0
CurrentType	RegSz	Multiprocessor Free
CurrentVersion	RegSz	6.3
EditionID	RegSz	ProfessionalEducation
EditionSubstring	RegSz	
InstallationType	RegSz	Client
InstallDate	RegDword	1548541202
ProductName	RegSz	Windows 10 Pro
ReleaseId	RegSz	1709
SoftwareType	RegSz	System
UBR	RegDword	967
PathName	RegSz	C:\Windows
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-37-38-2D-36-30-34-31-39-2D-37-37-37-34-37-
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-00-33-00-36-00-31-00-32-00-2D-00-30-00-33-00-37-
ProductId	RegSz	00378-60419-77747-AA664
RegisteredOwner	RegSz	Windows User
RegisteredOrganization	RegSz	
InstallTime	RegQword	131930148024847645

System information from registry - `SOFTWARE/Microsoft/Windows NT/CurrentVersion`

Product: Windows 10 Pro
Edition: Professional Education
Release ID: 1709
Build Number: 16299
Registered User: Windows User

Drag a column header here to group by that column

Value Name	Value Data
Bias	300
DaylightBias	-60
DaylightName	@tzres.dll,-111
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
StandardBias	0
StandardName	@tzres.dll,-112
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
TimeZoneKeyName	Eastern Standard Time
ActiveTimeBias	240

PROG-Wks03 Timezone information -
SYSTEM/ControlSet001/Control/TimeZoneInformation

Looking at the above values we can also see that the prog-wks03 system is in the same timezone as the it-wks01 system. This is due to the TimeZoneKeyName, Bias, DaylightBias, and ActiveTimeBias values.

Value Name	Value Type	Data
EnableDHCP	RegDword	1
Domain	RegSz	
DhcpIPAddress	RegSz	192.168.4.103
DhcpSubnetMask	RegSz	255.255.255.0
DhcpServer	RegSz	192.168.1.253
Lease	RegDword	691200
LeaseObtainedTime	RegDword	29
T1	RegDword	345629
T2	RegDword	604829
LeaseTerminatesTime	RegDword	691229
AddressType	RegDword	0
IsServerNapAware	RegDword	0
DhcpConnForceBroadcastFlag	RegDword	0
DhcpInterfaceOptions	RegBinary	FC-00-00-00-00-00-00-00-00-00-00-00-00-00-
DhcpDomain	RegSz	grru.local
DhcpNameServer	RegSz	192.168.1.254
DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0
DhcpDefaultGateway	RegMultiSz	192.168.4.1
DhcpGatewayHardware	RegBinary	C0-A8-04-01-06-00-00-00-00-0C-29-CF-28-C3
DhcpGatewayHardwareCount	RegDword	1

IT-wks01 Network information -
SYSTEM/ControlSet001/Services/Tcpip/Parameters/Interfaces/{4a13402c-0797-4b7a-b3c3-34dd88156587}

Last IP: 192.168.4.103/24
DNS Server: 192.168.1.254
Gateway: 192.168.4.1

DHCP Server: 192.168.1.253
DHCP Domain: grru.local

Valid...	User Name	Use...	Last Login Time	Total Login Count	Created On	In..
		=	=	=	=	=
☑	Administrator	500		0	2019-01-26 22:20:00	(
☑	Guest	501		0	2019-01-26 22:20:00	(
☑	DefaultAccount	503		0	2019-01-26 22:20:00	(
☑	WDAGUtilityAccount	504		0	2019-01-26 22:20:00	(
☑	TestLocal	1001	2019-01-26 23:53:33	3	2019-01-26 23:49:01	(

Prog-Wks03 accounts - `SAM\Domains\Account\Users`

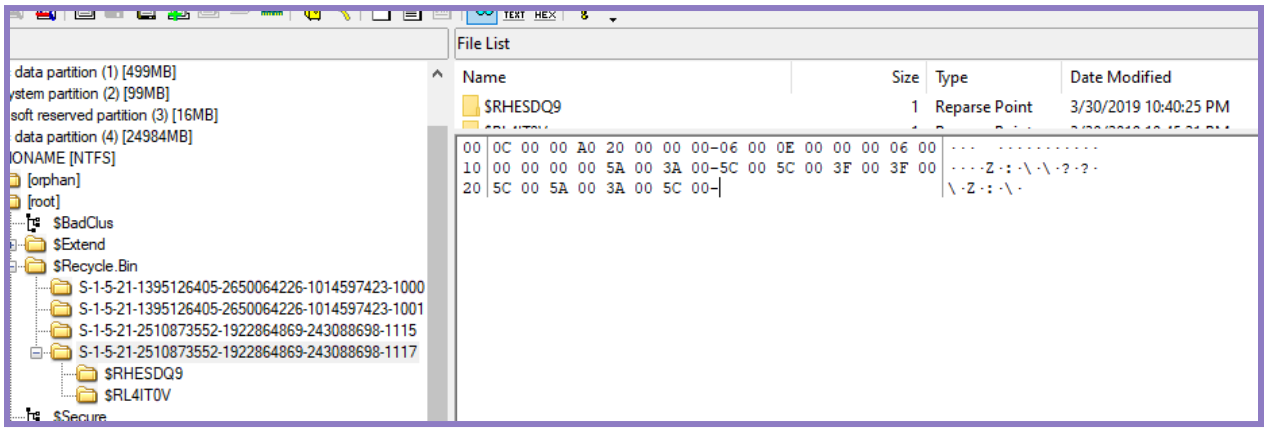
Drag a column header here to group by that column

Timestamp	Key Name	Profile Image Path
=		
2017-09-29 13:48:39	S-1-5-18	%systemroot%\system32\config\systemprofile
2019-01-26 22:13:26	S-1-5-19	C:\Windows\ServiceProfiles\LocalService
2019-01-26 22:13:21	S-1-5-20	C:\Windows\ServiceProfiles\NetworkService
2019-01-26 23:52:16	S-1-5-21-1395126405-2650064226-1014597423-1001	C:\Users\TestLocal
2019-02-23 19:57:23	S-1-5-21-2510873552-1922864869-243088698-1115	C:\Users\roger.melton
2019-02-14 07:14:02	S-1-5-21-2510873552-1922864869-243088698-1117	C:\Users\james.middleton-adm

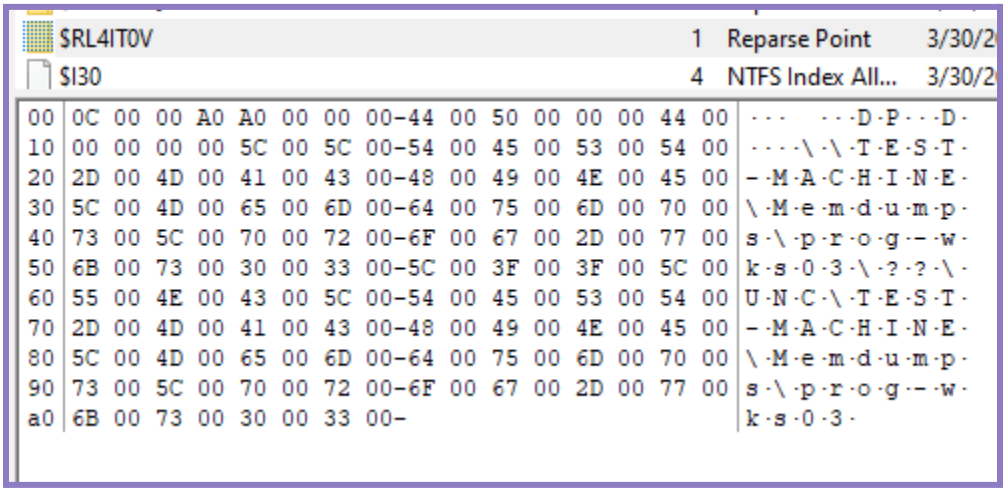
More user information including domain accounts - `SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`

For additional information on local user accounts see Appendix 4

Deleted Files



This screenshot shows the deleted files by james.middleton-adm on Prog-wks03. The file contents can be seen in the hex view.



This screenshot shows the other file that was deleted. It was a test file.

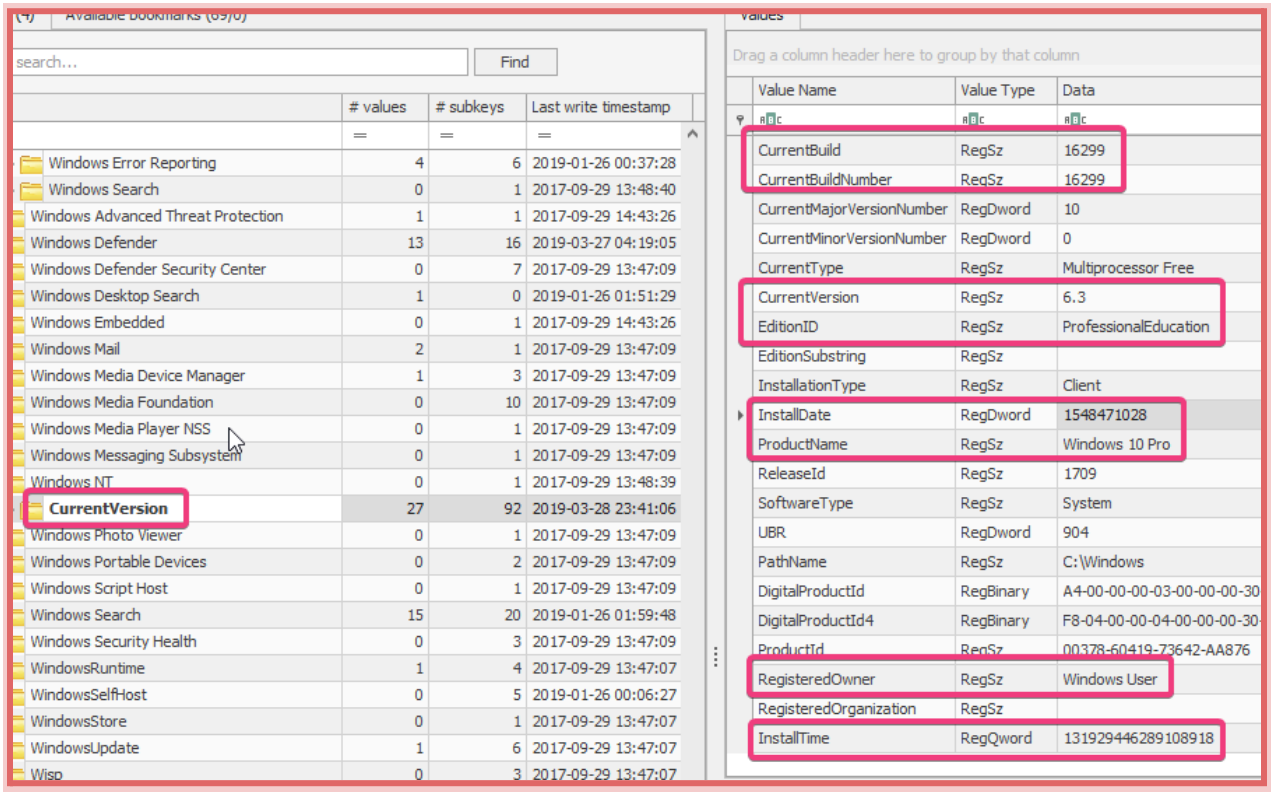
Installed Applications

Installed applications for It-wks01 and Prog-wks03 can be found in Appendix 1.

Files, Contacts, Chat rooms, Emails

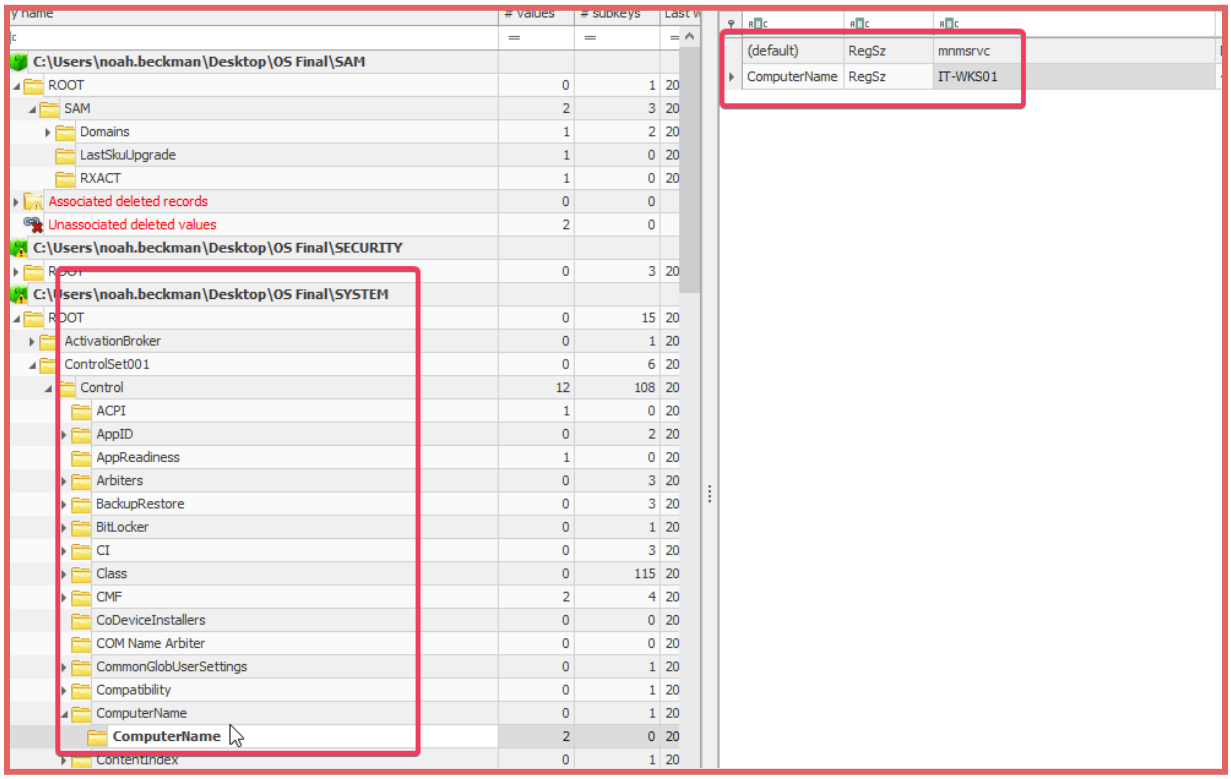
Information related to Emails, contacts, documents, contracts, source code, chatting, etc will be found in Appendix 2.

Computer Evidence analyzed



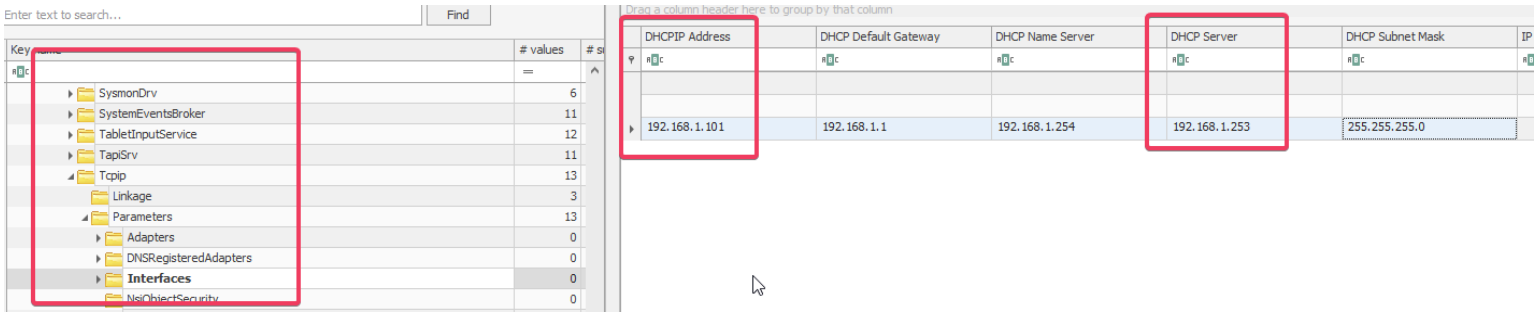
This screenshot shows system information for IT Workstation.

This information was found in the windows registry files for the device. It was specifically found in the SOFTWARE hive under the path `SOFTWARE/Microsoft/Windows NT/CurrentVersion`. It contains the OS, Version, Edition, Build number, install time, and registered owner. The install date was converted to traditional time: Install Date: *2019-01-26 02:50:28*



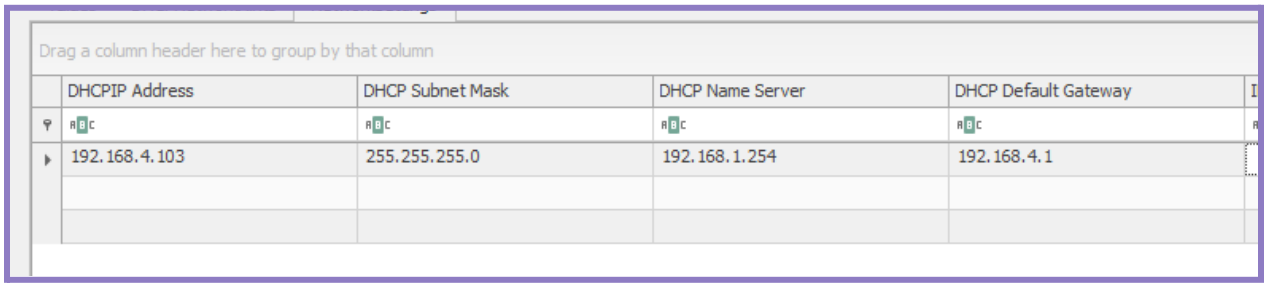
This Screenshot shows the computer name of IT-Workstation. This was found in the registry.

This screenshot shows the hostname of the computer. This was found using Registry Explorer in the SYSTEM hive under the path `SYSTEM/Controlset001/Control/ComputerName/ComputerName`



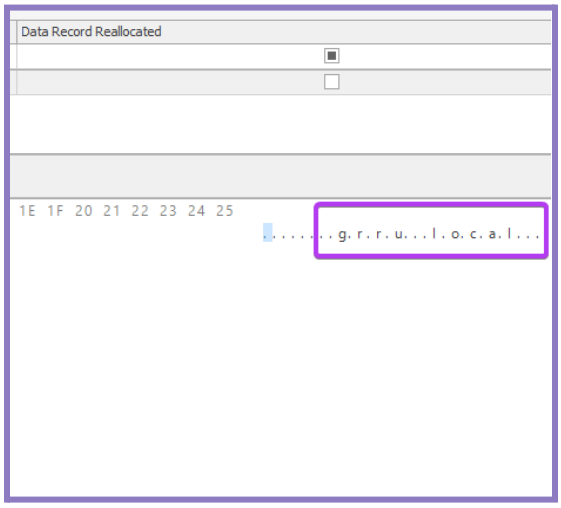
This screenshot shows the network information for IT Workstation

The network information in this screenshot was found in the SYSTEM hive under the path `SYSTEM/ControlSet001/Services/Tcpip/Parameters/Interfaces`



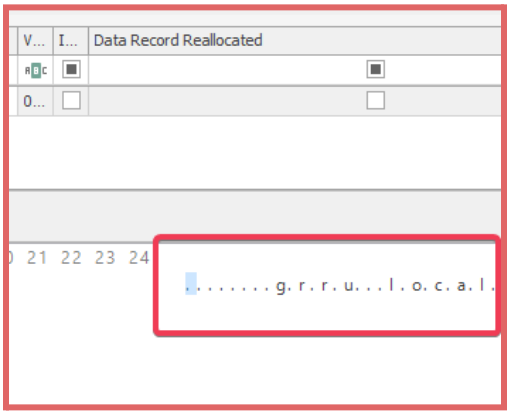
This screenshot shows the network information for prog-wks03

The network information from this screenshot was found using Registry Explorer inside the SYSTEM hive under the path `SYSTEM/ControlSet001/Services/Tcpip/Parameters/Interfaces`.



This screenshot shows the domain name that IT Workstation is joined to

This information was found in the SECURITY hive under the path `SECURITY\Policy\PolDnDDN`

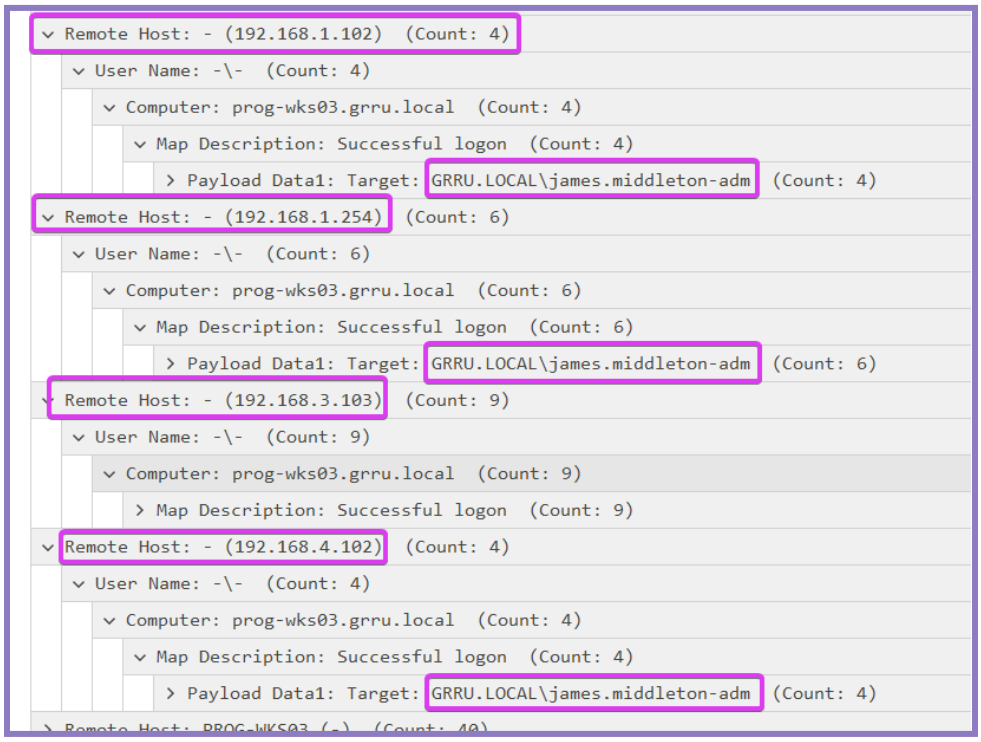


This screenshot shows similar domain information but for prog-wks3

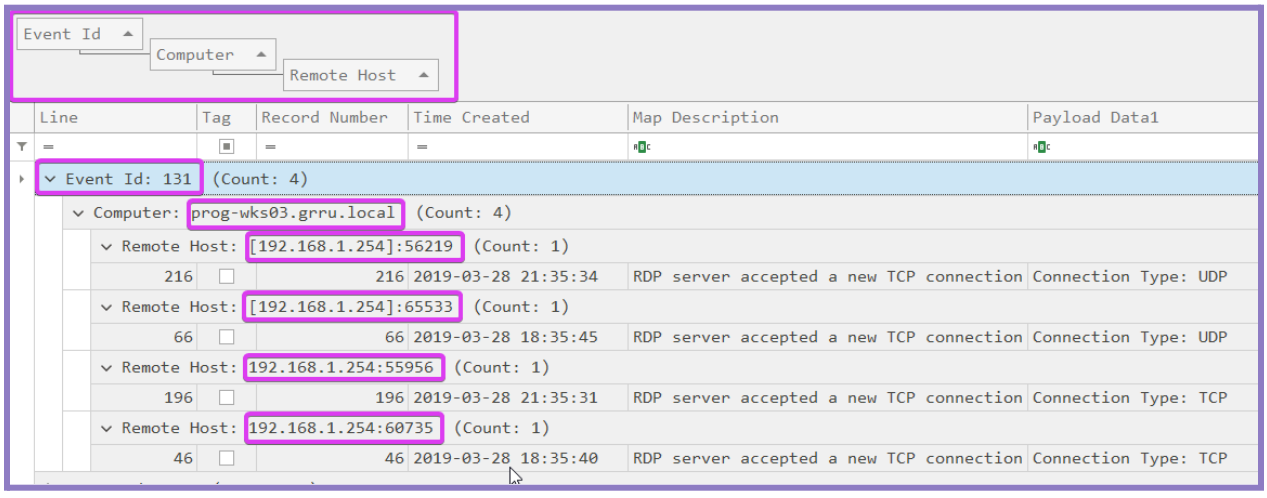
We can use this information to determine where the connection for file sharing purposes occurred. The following artifacts can be correlated together to show that both computers exist on the same network and domain. We can use the information presented above to analyze event logs containing network information for the first two reported issues from the network monitoring system.

Investigation Findings

Remote Login to Workstation



The network monitoring system detected a remote login to Prog-wks03. The screenshot above shows remote logins to prog from various other IPs that are not IT-wks01. Each one of these login attempts was by the user james.middleton-adm.



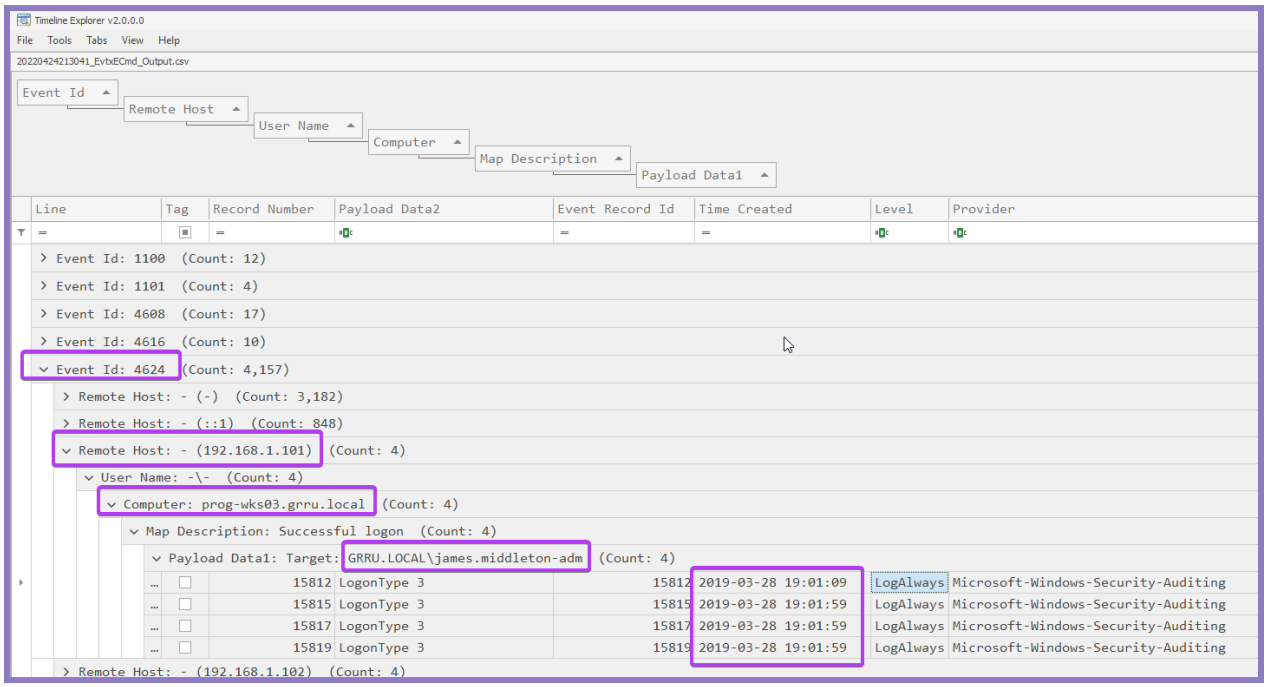
Other remote connections taken into consideration are provided in the screenshot above. On the suspected date there were 4 different tcp and udp connections made to Prog. For more information on remote connections see Appendix 5.

4648	1/26/2019 11:55:20 PM	Outgoing	A logon was attempted using explicit credentials.	TestLocal	PROG-WKS03	roger.melton	GRRU.LOCAL	
4648	1/26/2019 11:55:22 PM	Outgoing	A logon was attempted using explicit credentials.	TestLocal	PROG-WKS03	roger.melton	GRRU.LOCAL	192.168.1.254
4648	1/26/2019 11:55:23 PM	Outgoing	A logon was attempted using explicit credentials.	TestLocal	PROG-WKS03	roger.melton	GRRU.LOCAL	
4648	1/26/2019 11:55:23 PM	Outgoing	A logon was attempted using explicit credentials.	TestLocal	PROG-WKS03	roger.melton	GRRU.LOCAL	192.168.1.254

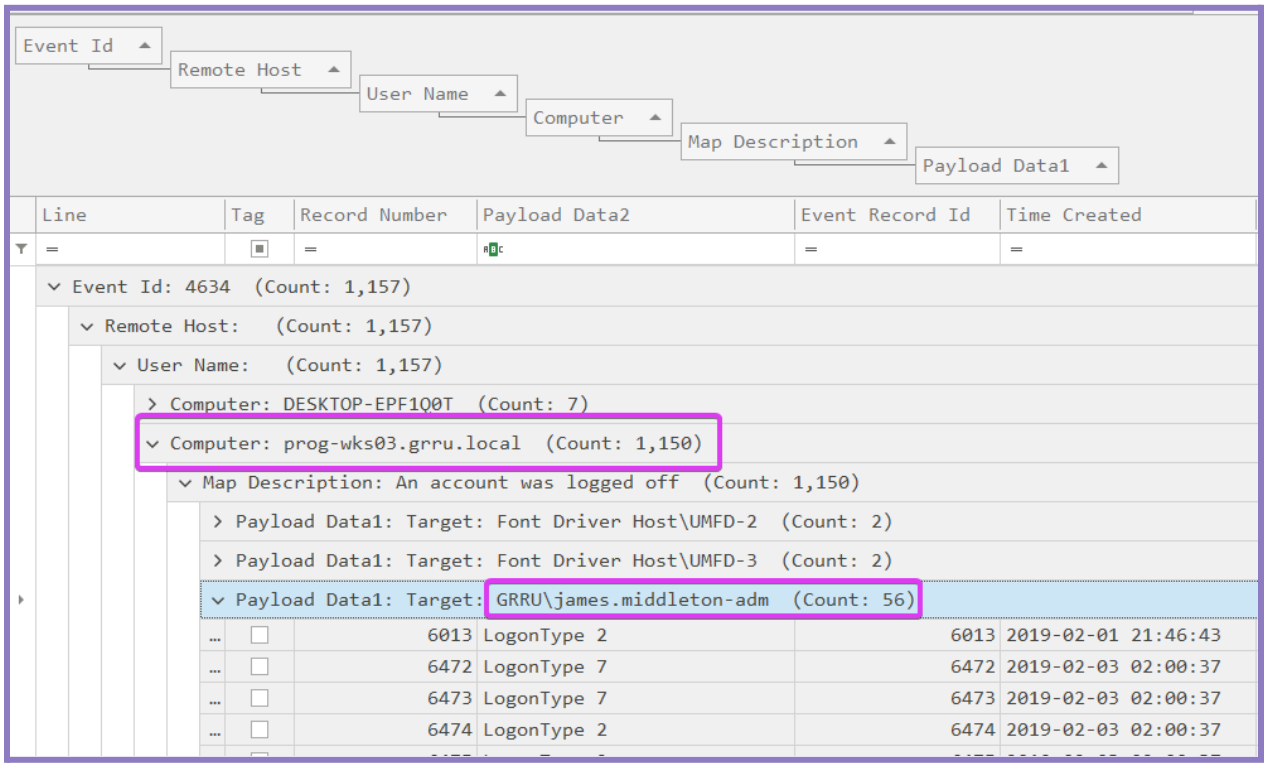
This screenshot shows another attempt to connect to prog by roger.melton

File/Network Share Connection

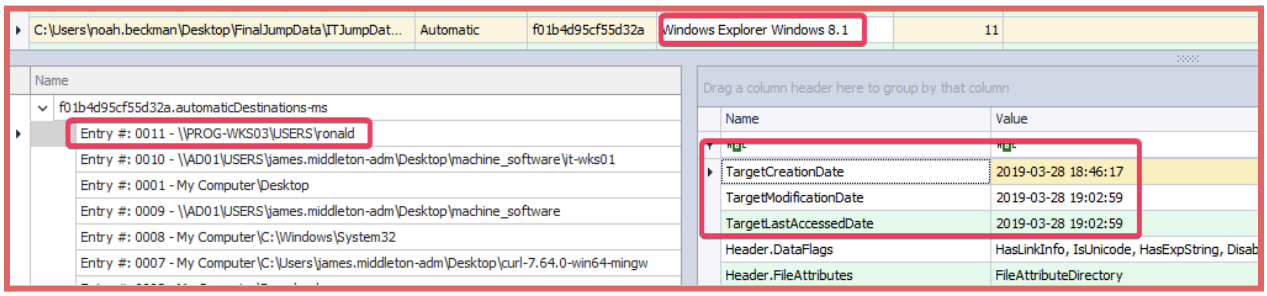
After analyzing windows event logs for account logins by remote host, I was able to find the connection that was used for file sharing.



This is a windows event system security log from prog-wks3. Event Id 4624 is a number designated to the event where an account was successfully logged into. As detailed in a previous screenshot, IT workstation's ip is 192.168.1.101. This can be seen as the remote host above that is being connected to. The computer IT workstation was trying to connect to was prog-wks03. We can see the user that was trying to connect: james.middleton-adm. Lastly we can see the times when the login occurred.

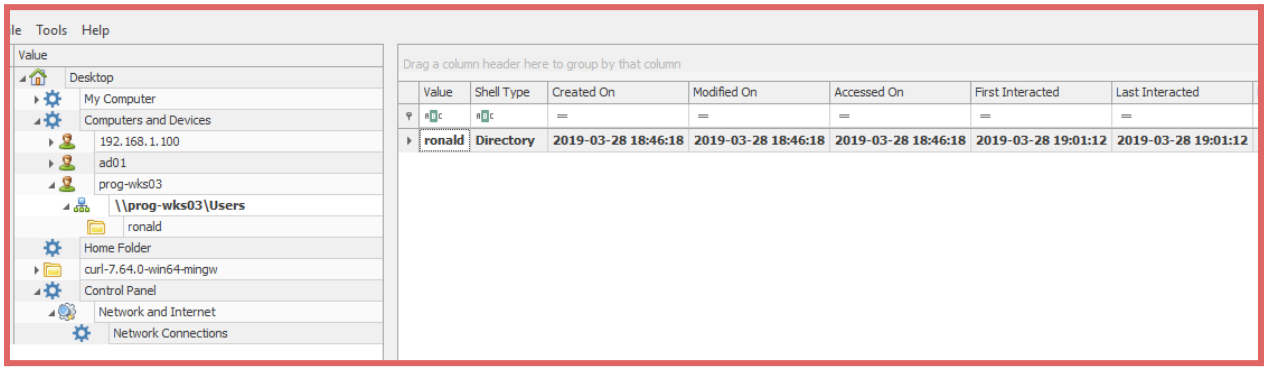


You can also determine from another event log that logs user logouts when the user that logged in left. This can be found in the security log and is event id 4634. This will help create a timeline of events later on.



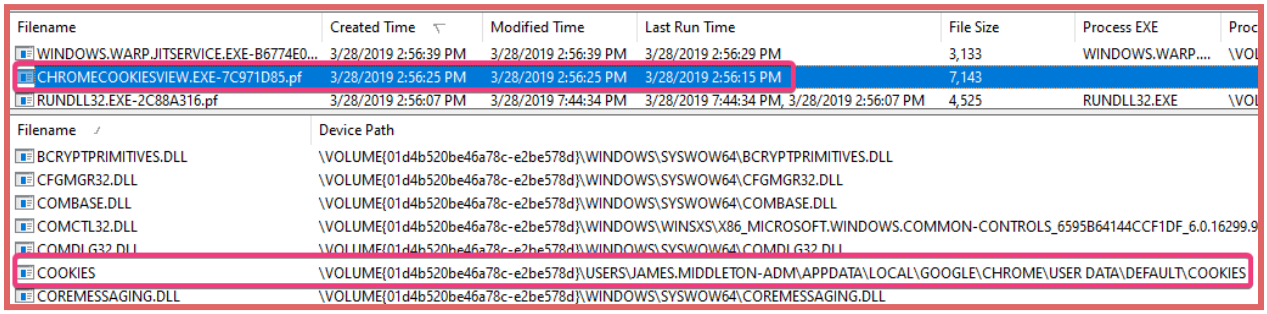
Jumplist file showing Connection to Prog-wks03 as a network share

Another supporting artifact of this connection is the following jumplist entry that shows the user James.middleton-adm accessing PROG-WKS03 specifically targeting the \USERS\ronald directory. This is important because this location is where the data exfiltration was placed.



This directory can also be seen in the shellbag file located in james.middleton-adm's Userclass.dat file on It-wks01.

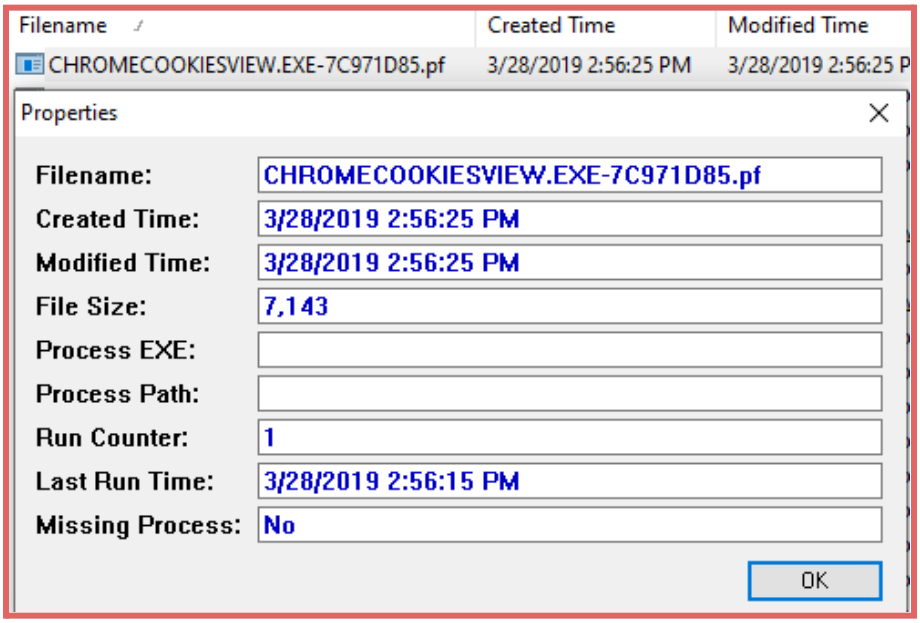
Outgoing Connection with Data Exfiltration



Filename	Created Time	Modified Time	Last Run Time	File Size	Process EXE	Proc
WINDOWS.WARP.JITSERVICE.EXE-B6774E0...	3/28/2019 2:56:39 PM	3/28/2019 2:56:39 PM	3/28/2019 2:56:29 PM	3,133	WINDOWS.WARP....	\VOL
CHROMECOOKIESVIEW.EXE-7C971D85.pf	3/28/2019 2:56:25 PM	3/28/2019 2:56:25 PM	3/28/2019 2:56:15 PM	7,143		
RUNDLL32.EXE-2C88A316.pf	3/28/2019 2:56:07 PM	3/28/2019 7:44:34 PM	3/28/2019 7:44:34 PM, 3/28/2019 2:56:07 PM	4,525	RUNDLL32.EXE	\VOL

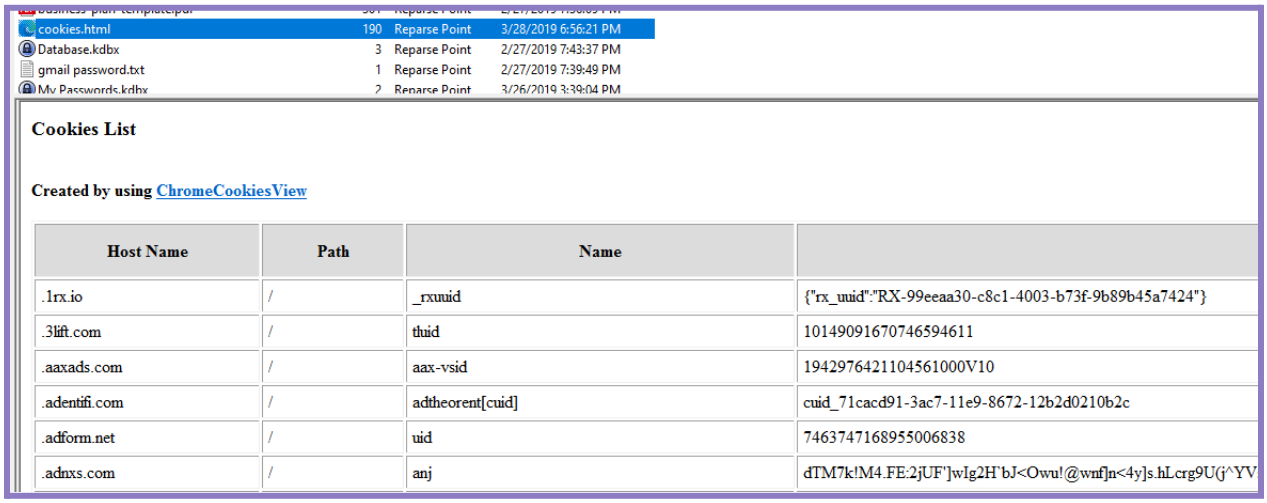
Filename	Device Path
BCRYPTPRIMITIVES.DLL	\VOLUME{01d4b520be46a78c-e2be578d}\WINDOWS\SYSWOW64\BCRYPTPRIMITIVES.DLL
CFGMGR32.DLL	\VOLUME{01d4b520be46a78c-e2be578d}\WINDOWS\SYSWOW64\CFGMGR32.DLL
COMBASE.DLL	\VOLUME{01d4b520be46a78c-e2be578d}\WINDOWS\SYSWOW64\COMBASE.DLL
COMCTL32.DLL	\VOLUME{01d4b520be46a78c-e2be578d}\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-CONTROLS_6595B64144CCF1DF_6.0.16299.9
COMDLG32.DLL	\VOLUME{01d4b520be46a78c-e2be578d}\WINDOWS\SYSWOW64\COMDLG32.DLL
COOKIES	\VOLUME{01d4b520be46a78c-e2be578d}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\DEFAULT\COOKIES
COREMESSAGING.DLL	\VOLUME{01d4b520be46a78c-e2be578d}\WINDOWS\SYSWOW64\COREMESSAGING.DLL

This screenshot shows the application chromecookiesview.exe being run once. The data was viewed using WinPrefetchView. This application allows a user to display all the cookies stored by Google chrome and delete cookies you don't want to be found. You can also export your own cookies to a csv file. This is important to data exfiltration as one of the users chrome cookies was exfiltrated.

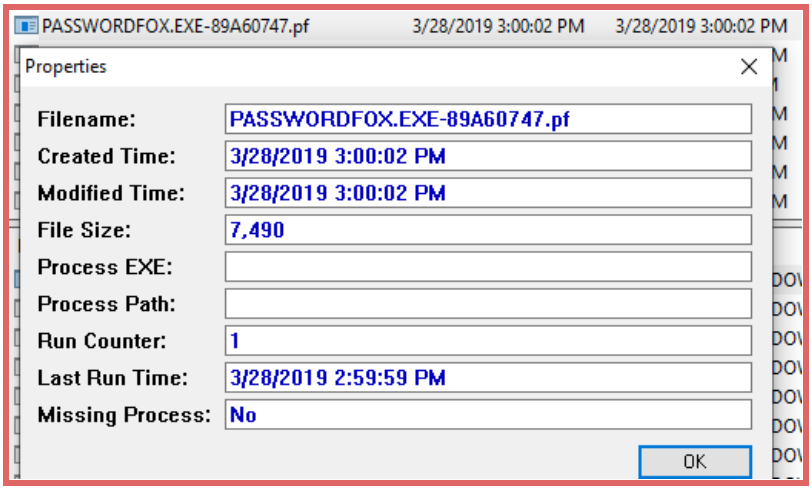


This is the information page of the chromecookiesview entry.

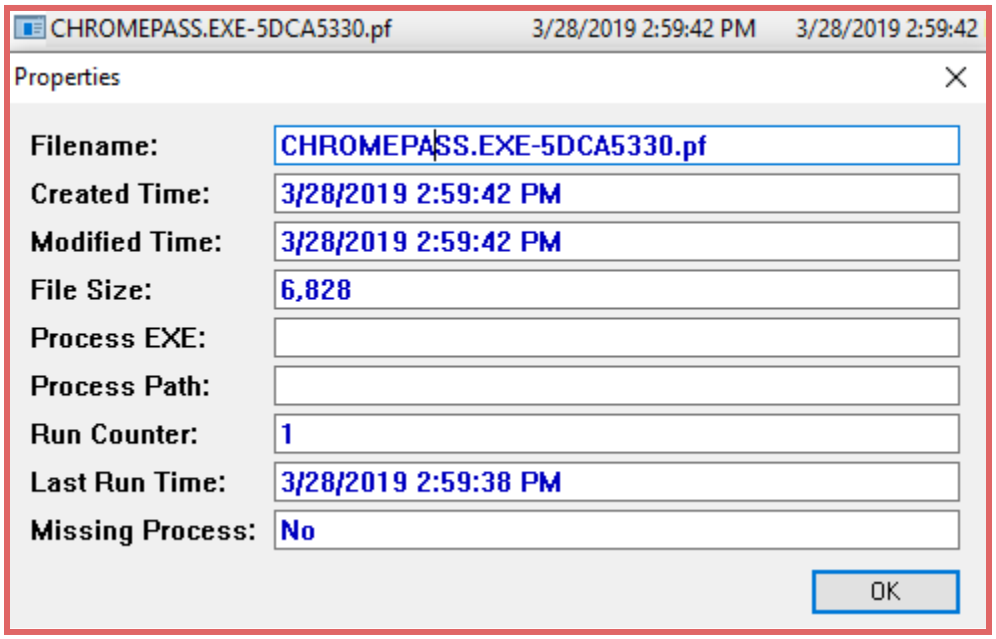
This screenshot shows more specific information regarding the application. It informs us about the created, modified, and last run times as well as how many times it was run. This information allows us to plot on the timeline when this event occurred.



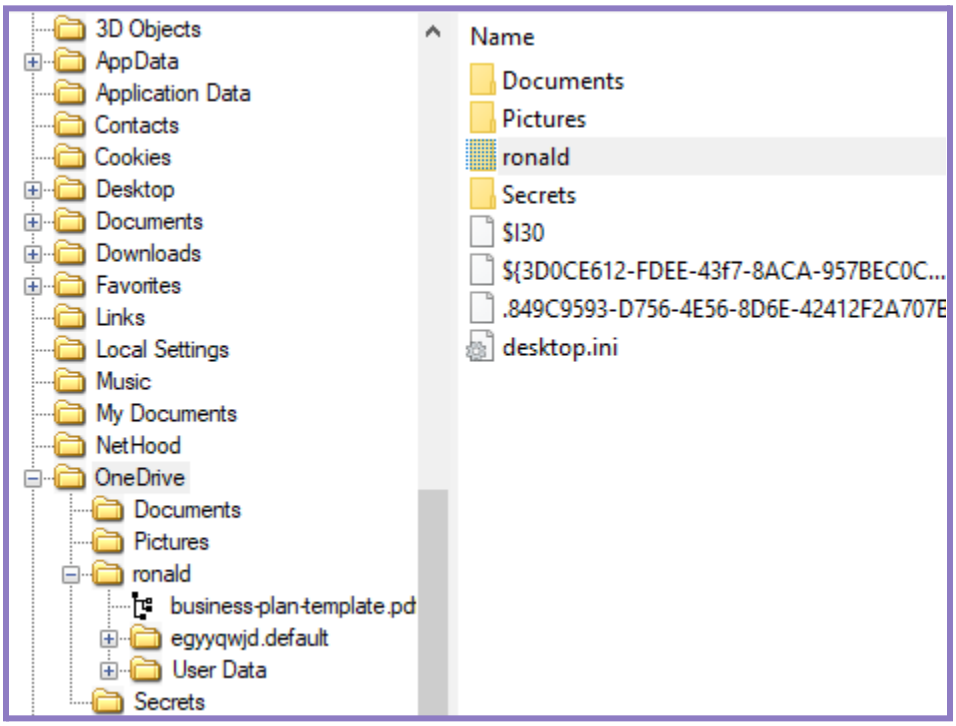
This is a screenshot of the exfiltrated cookie data.



Another malicious program that was run is Passwordfox.exe. Password fox is a lightweight utility that detects what passwords firefox has stored in memory and displays them with associated information.



Chromepass.exe is another malicious program that was run on IT workstation. This program is a password recovery tool that allows you to view the user names and passwords stored by Google Chrome.

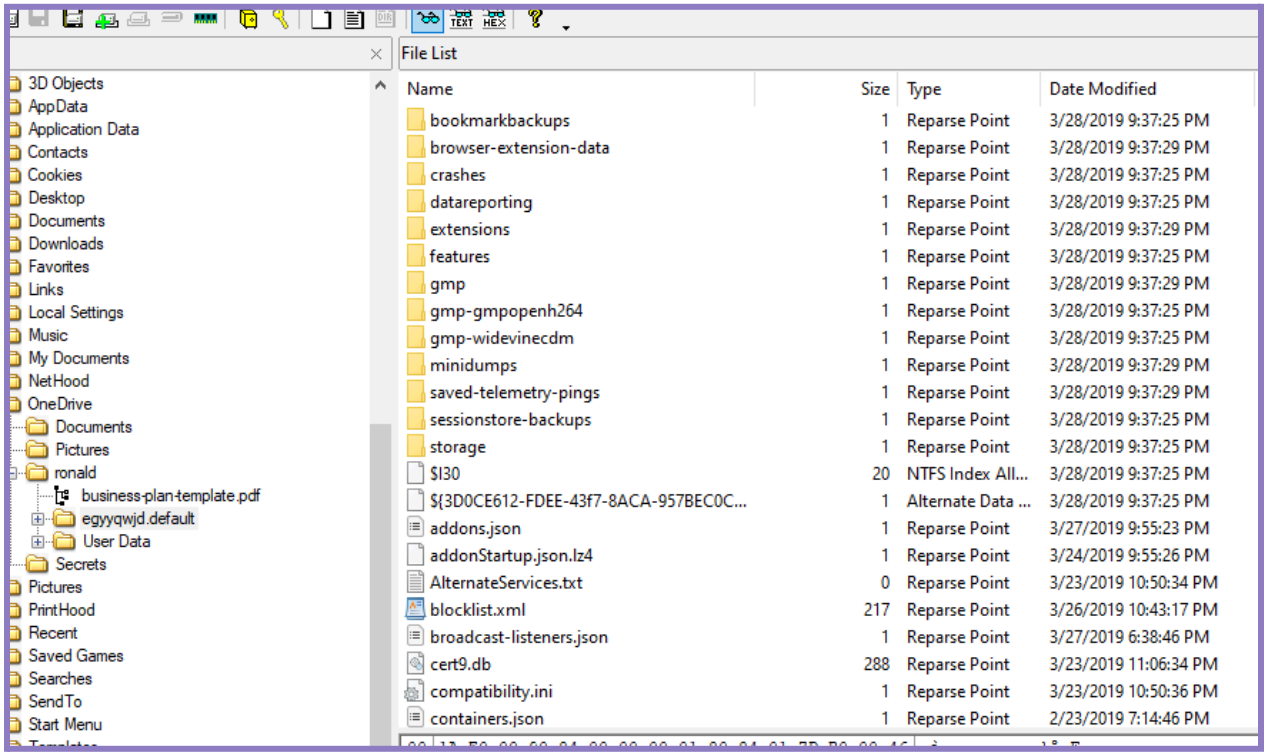


This screenshot shows the folder in where the data was exfiltrated to on Prog-Wks03

As we saw in the shellbag, the folder ronald is where the data was being moved too. This can be found under C:/Users/James.Middleton-adm/OneDrive/ronald.

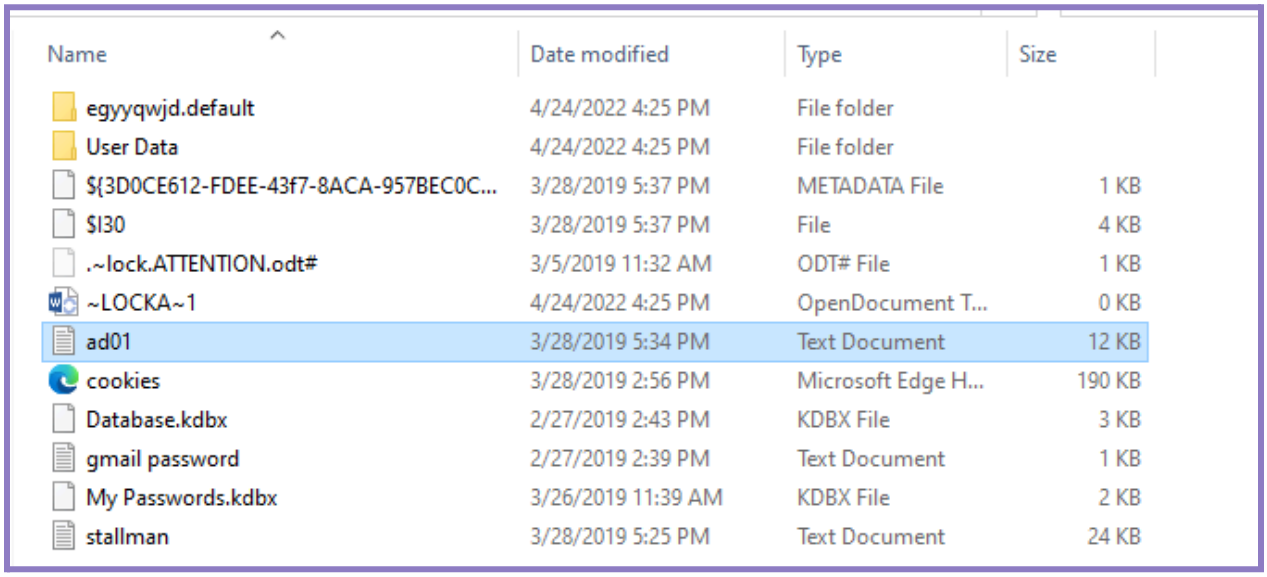
Name	Size	Type	Date Modified
BrowserMetrics	1	Reparse Point	3/28/2019 9:37:25 PM
CertificateRevocation	1	Reparse Point	3/28/2019 9:37:25 PM
CertificateTransparency	1	Reparse Point	3/28/2019 9:37:25 PM
Crashpad	1	Reparse Point	3/28/2019 9:37:25 PM
Default	1	Reparse Point	3/28/2019 9:37:25 PM
FileTypePolicies	1	Reparse Point	3/28/2019 9:37:25 PM
InterventionPolicyDatabase	1	Reparse Point	3/28/2019 9:37:25 PM
MEIPreload	1	Reparse Point	3/28/2019 9:37:29 PM
OriginTrials	1	Reparse Point	3/28/2019 9:37:29 PM
PepperFlash	1	Reparse Point	3/28/2019 9:37:25 PM
pnacl	1	Reparse Point	3/28/2019 9:37:25 PM
Safe Browsing	1	Reparse Point	3/28/2019 9:37:25 PM
ShaderCache	1	Reparse Point	3/28/2019 9:37:25 PM
SSLErrorAssistant	1	Reparse Point	3/28/2019 9:37:25 PM
Subresource Filter	1	Reparse Point	3/28/2019 9:37:26 PM
SwReporter	1	Reparse Point	3/28/2019 9:37:25 PM
WidevineCdm	1	Reparse Point	3/28/2019 9:37:29 PM
$I30	8	NTFS Index All...	3/28/2019 9:37:25 PM
${3D0CE612-FDEE-43f7-8ACA-957BEC0C...	1	Alternate Data ...	3/28/2019 9:37:25 PM
BrowserMetrics-spare.pma	4,096	Reparse Point	3/24/2019 9:03:37 PM
chrome_shutdown_ms.txt	1	Reparse Point	3/26/2019 9:33:37 PM
CrashpadMetrics-active.pma	1,024	Reparse Point	3/26/2019 9:33:20 PM
CrashpadMetrics.pma	1,024	Reparse Point	3/24/2019 9:04:30 PM

This screenshot shows the contents of the User Data folder that was exfiltrated. It contains a bunch of Chrome information.

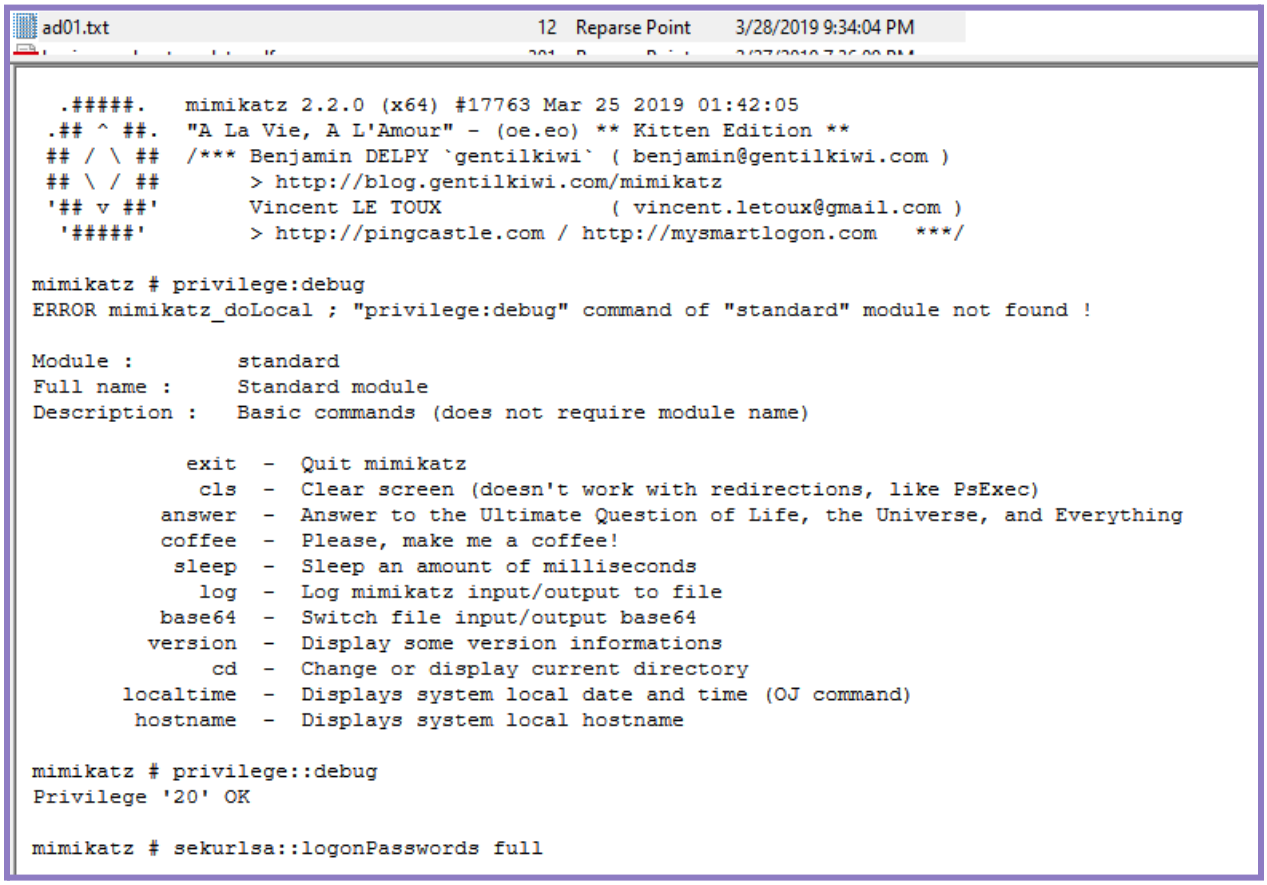


This screenshot shows the data contained in the egyyqwijd.default folder within the exfiltrated data. It contains information related to web browsers.

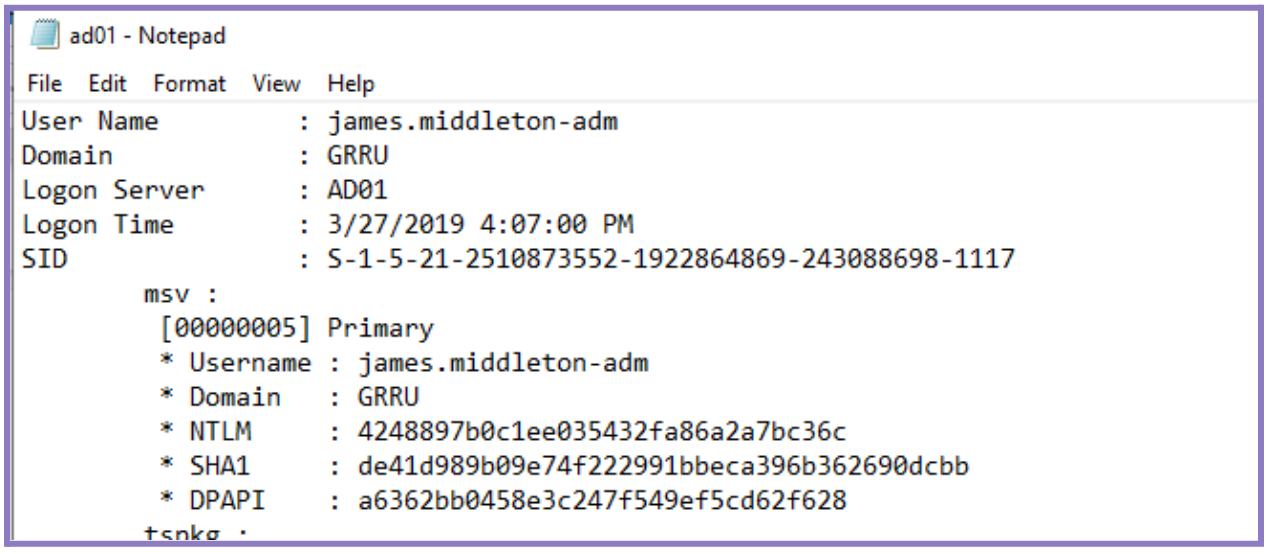
Cracked Password



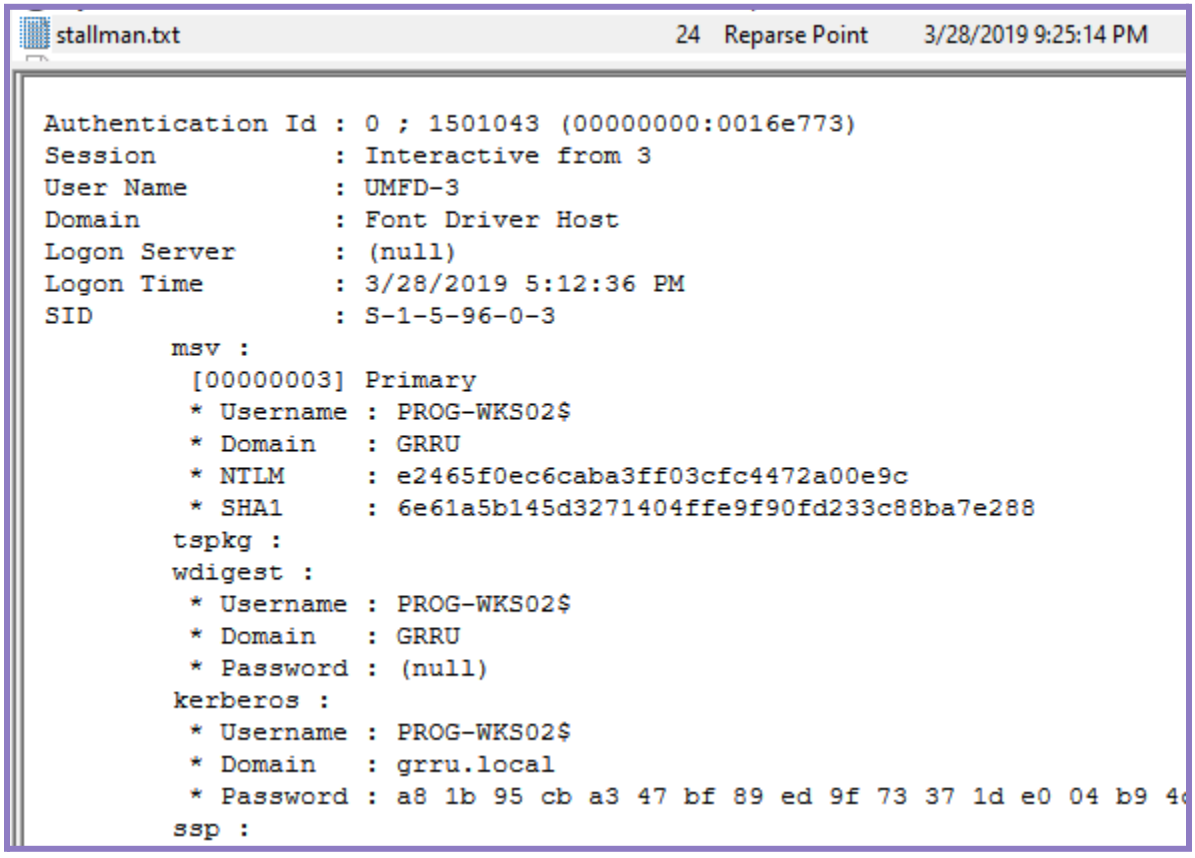
This screenshot shows all the data that was exfiltrated to Prog-wks03. The file that is highlighted named ad01 is actually a text document containing various password hashes that were stolen by the program mimikatz. The text file contains the output of the program.



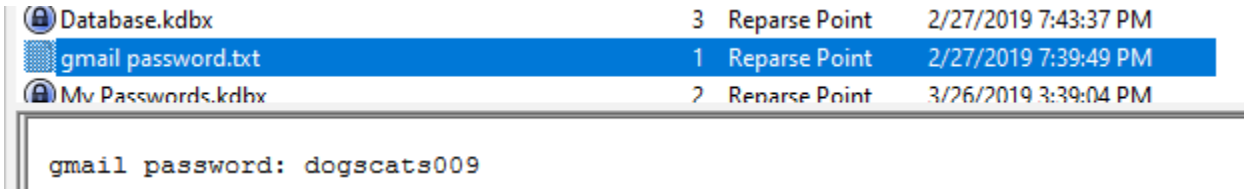
This is the output of the file. You can see that it is mimikatz version 2.2.0 and when it was run.



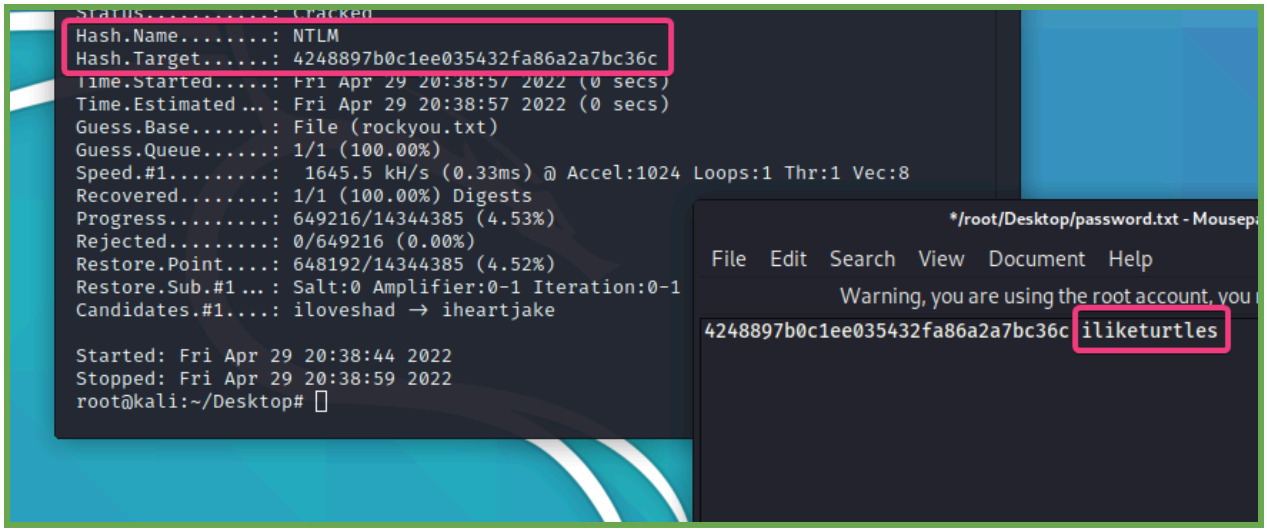
This is one of the users that was captured. James.middleton-adm's domain account password has been stolen. This text file only contains the hash. However, the password is not secure and easy to crack.



This screenshot shows the output of the file stallman.txt. This is another mimikatz output file.



This screenshot shows james.middleton-adm's gmail password. He left this file on his desktop and it was exfiltrated with the rest of the information in the directory.



This screenshot shows me cracking james-middleton-adm's domain account password. I used a kali vm and the program hashcat to test his password hash against the rockyou wordlist. Within seconds the hash was cracked.

Timeline

Event	Artifact Source	Time
Mimikatz run	File data	2019-03-25 01:42:05
ChromeCookiesView run	Prefetch - IT	2019-03-28 14:56:25
ChromePass.exe run	Prefetch - IT	2019-03-28 14:59:42
Password Fox.exe run	Prefetch - IT	2019-03-28 15:00:02
Data Exfiltration - database.kdbx	Exfiled Data	2019-03-28 15:01:41
Data Exfiltration - gmail password.txt	Exfiled Data	2019-03-28 15:01:59
Data Exfiltration - chrome cookies	Exfiled Data	2019-03-28 15:02:59
James.middleton-adm password compromise	File data	2019-03-28 16:07:00
Data Exfiltration - Firefox data (User Data)	Exfiled Data	2019-03-28 17:10:27
Mimikatz run	File data	2019-03-28 17:12:36
Data Exfiltration - Chrome data (egyyqwjd.default)	Exfiled Data	2019-03-28 17:18:21
Data Exfiltration - My Passwords.kbdx	Exfiled Data	2019-03-28 17:25:53
Data Exfiltration - stallman.txt	Exfiled Data	2019-03-28 17:25:53
Data Exfiltration - credentials / mimikatz output	Exfiled Data	2019-03-28 17:34:02
James.middleton-adm Logon to Prog from IT	Event Log - Prog	2019-03-28 19:01:09
Ronald folder first interacted	Shellbag - IT	2019-03-28 19:01:12
James.middleton-adm Log off	Event Log - Prog	2019-03-28 19:01:59

from Prog		
ronald folder access	Jumplist - IT	2019-03-28 19:02:59
James.middleton-adm Log off from Prog	Event Log - Prog	2019-03-28 19:05:21

Executive Summary

The objective of this investigation was to find out what information might have been compromised, leaked, or stolen. In addition, determining where remote connections, file sharing, and data exfiltration occurred. The timeline above illustrates the artifacts explained in the order in which they occurred to attempt to outline the found artifacts and deliver on the objectives. At minimum, four separate applications that were malicious were run on IT-wks01. Each of these were run with the intent to harvest data and extract information. The data was then copied to a folder, ronald, then a remote connection was made to Prog-wks3 and the files were transferred to a Onedrive directory. I would recommend asking James Middleton what he was doing collecting files and passwords. If it was not him, determining who gained access to his account is critical.

Appendix

1 - Installed Applications

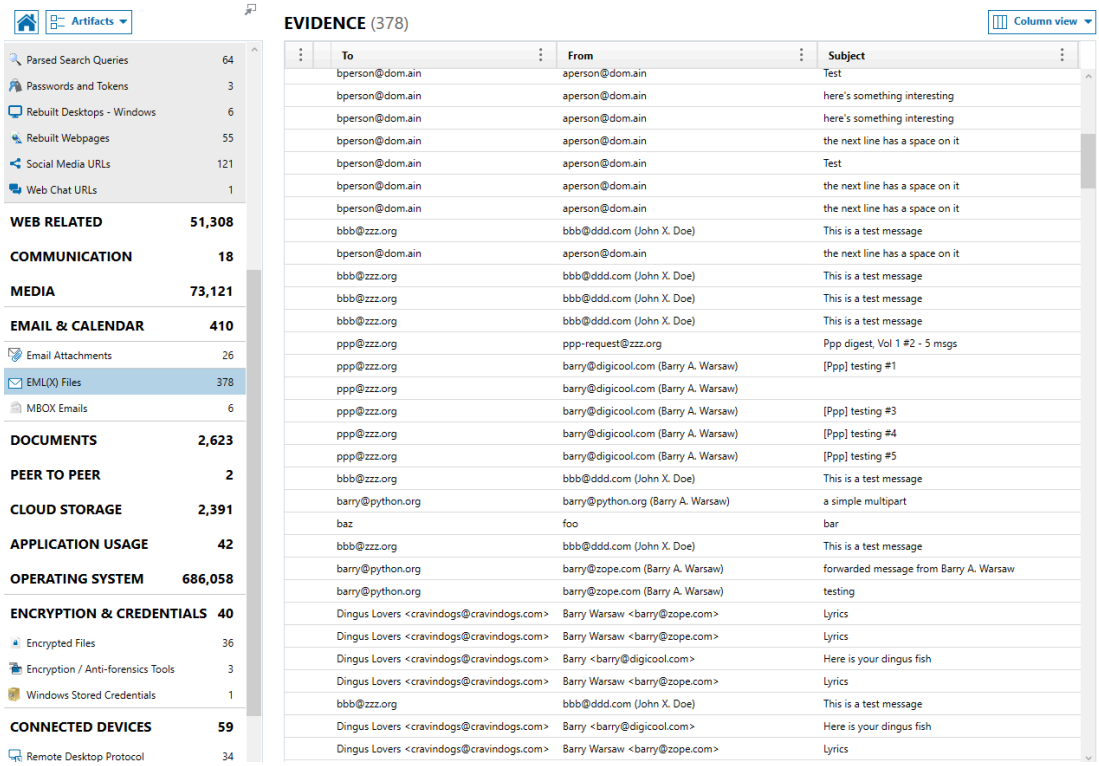
C:\Users\noah.beckman\Desktop\OS Final\SOFTWARE: Microsoft\Windows\CurrentVersion\App Paths

Application Name	Version	Created Date	Source	Company
Spotify	1.1.2.285.ga97985ef	3/28/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Users\james.middleton-adm\NTUSER.DAT	Spotify AB
7-Zip 18.06 (x64)	18.06		it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Igor Pavlov
GIMP 2.10.8	2.10.8	2/14/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	The GIMP Team
VLC media player	3.0.6		it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	VideoLAN
PuTTY release 0.70 (64-bit)	0.70.0.0	2/14/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Simon Tatham
Google Chrome	73.0.3683.86	2/14/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Google LLC
Dropbox	69.4.102		it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Dropbox, Inc.
AccessData FTK Imager	4.2.0.13	3/28/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	AccessData

KeePass Password Safe 2.41	2.41	2/14/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Dominik Reichl
Notepad++ (32-bit x86)	7.6.3		it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Notepad++ Team
Skype version 8.41	8.41	3/20/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Skype Technologies S.A.
TeamViewer 14	14.1.9025		it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	TeamViewer
WinSCP 5.13.7	5.13.7	2/14/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Martin Prikryl
Dropbox Update Helper	1.3.189.1	2/14/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Dropbox, Inc.
Python 2.7.15	2.7.15150	2/14/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Python Software Foundation
Java(TM) 6 Update 22	6.0.220	1/26/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Oracle
OpenOffice.org 3.3	3.3.9567	1/26/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	OpenOffice.org
Java Auto Updater	2.0.2.4	1/26/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Sun Microsystems, Inc.
Google Update Helper	1.3.34.7	3/27/2019	it-wks01.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE	Google LLC
7-Zip 18.06 (x64)	18.06		prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	Igor Pavlov

GIMP 2.10.8	2.10.8	2/17/2019	prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	The GIMP Team
Git version 2.20.1	2.20.1	2/23/2019	prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	The Git Development Community
Mozilla Firefox 66.0.1 (x64 en-US)	66.0.1		prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	Mozilla
Mozilla Maintenance Service	65.0.1		prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	Mozilla
AccessData FTK Imager	4.2.0.13	3/28/2019	prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	Mozilla
IrfanView 4.52 (32-bit)	4.52		prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	Irfan Skiljan
Notepad++ (32-bit x86)	7.6.3		prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	Notepad++ Team
OpenOffice 4.1.6	4.16.9790	2/1/2019	prog-wks03.E01 - Partition 4 (Microsoft NTFS, 24.4 GB)\Windows\System32\config\SOFTWARE	Apache Software Foundation

2 - Files, Contacts, Chat rooms, Emails



Artifacts

Parsed Search Queries	64
Passwords and Tokens	3
Rebuilt Desktops - Windows	6
Rebuilt Webpages	55
Social Media URLs	121
Web Chat URLs	1
WEB RELATED	**51,308**
COMMUNICATION	**18**
MEDIA	**73,121**
EMAIL & CALENDAR	**410**
Email Attachments	26
EML(X) Files	378
MBOX Emails	6
DOCUMENTS	**2,623**
PEER TO PEER	**2**
CLOUD STORAGE	**2,391**
APPLICATION USAGE	**42**
OPERATING SYSTEM	**686,058**
ENCRYPTION & CREDENTIALS	**40**
Encrypted Files	36
Encryption / Anti-forensics Tools	3
Windows Stored Credentials	1
CONNECTED DEVICES	**59**
Remote Desktop Protocol	34

EVIDENCE (378) — Column view

To	From	Subject
bperson@dom.ain	aperson@dom.ain	Test
bperson@dom.ain	aperson@dom.ain	here's something interesting
bperson@dom.ain	aperson@dom.ain	here's something interesting
bperson@dom.ain	aperson@dom.ain	the next line has a space on it
bperson@dom.ain	aperson@dom.ain	Test
bperson@dom.ain	aperson@dom.ain	the next line has a space on it
bperson@dom.ain	aperson@dom.ain	the next line has a space on it
bbb@zzz.org	bbb@ddd.com (John X. Doe)	This is a test message
bperson@dom.ain	aperson@dom.ain	the next line has a space on it
bbb@zzz.org	bbb@ddd.com (John X. Doe)	This is a test message
bbb@zzz.org	bbb@ddd.com (John X. Doe)	This is a test message
bbb@zzz.org	bbb@ddd.com (John X. Doe)	This is a test message
ppp@zzz.org	ppp-request@zzz.org	Ppp digest, Vol 1 #2 - 5 msgs
ppp@zzz.org	barry@digicool.com (Barry A. Warsaw)	[Ppp] testing #1
ppp@zzz.org	barry@digicool.com (Barry A. Warsaw)	
ppp@zzz.org	barry@digicool.com (Barry A. Warsaw)	[Ppp] testing #3
ppp@zzz.org	barry@digicool.com (Barry A. Warsaw)	[Ppp] testing #4
ppp@zzz.org	barry@digicool.com (Barry A. Warsaw)	[Ppp] testing #5
bbb@zzz.org	bbb@ddd.com (John X. Doe)	This is a test message
barry@python.org	barry@python.org (Barry A. Warsaw)	a simple multipart
baz	foo	bar
bbb@zzz.org	bbb@ddd.com (John X. Doe)	This is a test message
barry@python.org	barry@zope.com (Barry A. Warsaw)	forwarded message from Barry A. Warsaw
barry@python.org	barry@zope.com (Barry A. Warsaw)	testing
Dingus Lovers <cravindogs@cravindogs.com>	Barry Warsaw <barry@zope.com>	Lyrics
Dingus Lovers <cravindogs@cravindogs.com>	Barry Warsaw <barry@zope.com>	Lyrics
Dingus Lovers <cravindogs@cravindogs.com>	Barry <barry@digicool.com>	Here is your dingus fish
Dingus Lovers <cravindogs@cravindogs.com>	Barry Warsaw <barry@zope.com>	Lyrics
bbb@zzz.org	bbb@ddd.com (John X. Doe)	This is a test message
Dingus Lovers <cravindogs@cravindogs.com>	Barry <barry@digicool.com>	Here is your dingus fish
Dingus Lovers <cravindogs@cravindogs.com>	Barry Warsaw <barry@zope.com>	Lyrics

Emails none are relevant as the timeframe from them is out of scope.

Messaging Applications:

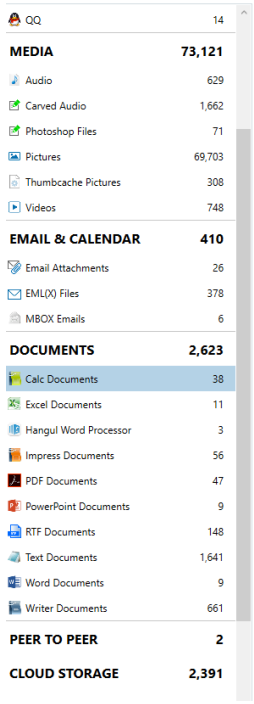
Google hangouts

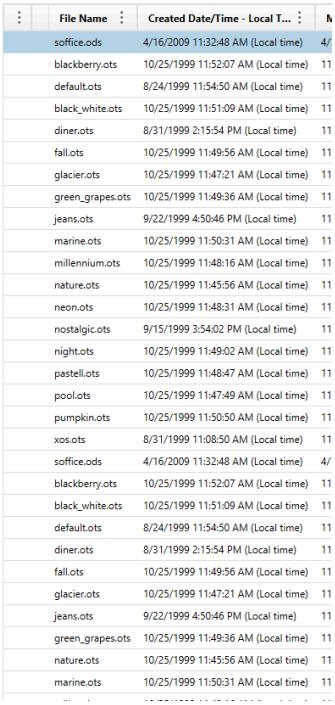
Chrome / Edge / Firefox search terms

Keyword Searc...	URL	Last Visited D...	Artifact type	Source
programming guides	https://www.google.com/search?tbm=isch&source=...	2/27/2019 7:33:33 PM	Chrome Keyword Search Terms	it-wks01.E01
programming guides	https://www.google.com/search?q=programming+g...	2/27/2019 7:33:37 PM	Chrome Keyword Search Terms	it-wks01.E01
programming books	https://www.google.com/search?biw=988&bih=620...	2/27/2019 7:33:39 PM	Chrome Keyword Search Terms	it-wks01.E01
awesome list github	https://www.google.com/search?q=awesome+list+g...	2/27/2019 7:34:04 PM	Chrome Keyword Search Terms	it-wks01.E01
intel handbook	https://www.google.com/search?source=hp&ei=Mu...	2/27/2019 7:34:55 PM	Chrome Keyword Search Terms	it-wks01.E01
how to get free v bucks	https://www.google.com/search?q=how+to+get+fr...	2/27/2019 7:35:51 PM	Chrome Keyword Search Terms	it-wks01.E01
how to get free money	https://www.google.com/search?rlz=1C1GCEA_enUS...	2/27/2019 7:35:54 PM	Chrome Keyword Search Terms	it-wks01.E01
business plan pdf	https://www.google.com/search?rlz=1C1GCEA_enUS...	2/27/2019 7:36:00 PM	Chrome Keyword Search Terms	it-wks01.E01
free wallpapers	https://www.google.com/search?q=free+wallpapers...	2/27/2019 7:44:13 PM	Chrome Keyword Search Terms	it-wks01.E01
curl for windows	https://www.google.com/search?q=curl+for+windo...	3/1/2019 5:16:52 PM	Chrome Keyword Search Terms	it-wks01.E01
sysmon	https://www.google.com/search?q=sysmon&rlz=1C...	3/20/2019 2:17:04 AM	Chrome Keyword Search Terms	it-wks01.E01

Emails none are relevant as the timeframe from them is out of scope.
Social media applications - Twitter, LinkedIn, Reddit,

Documents





File Name	Created Date/Time - Local T...	M
soffice.ods	4/16/2009 11:32:48 AM (Local time)	4/
blackberry.ots	10/25/1999 11:52:07 AM (Local time)	11
default.ots	8/24/1999 11:54:50 AM (Local time)	11
black_white.ots	10/25/1999 11:51:09 AM (Local time)	11
diner.ots	8/31/1999 2:15:54 PM (Local time)	11
fall.ots	10/25/1999 11:49:56 AM (Local time)	11
glacier.ots	10/25/1999 11:47:21 AM (Local time)	11
green_grapes.ots	10/25/1999 11:49:36 AM (Local time)	11
jeans.ots	9/22/1999 4:50:46 PM (Local time)	11
marine.ots	10/25/1999 11:50:31 AM (Local time)	11
millennium.ots	10/25/1999 11:48:16 AM (Local time)	11
nature.ots	10/25/1999 11:45:56 AM (Local time)	11
neon.ots	10/25/1999 11:48:31 AM (Local time)	11
nostalgic.ots	9/15/1999 3:54:02 PM (Local time)	11
night.ots	10/25/1999 11:49:02 AM (Local time)	11
pastell.ots	10/25/1999 11:48:47 AM (Local time)	11
pool.ots	10/25/1999 11:47:49 AM (Local time)	11
pumpkin.ots	10/25/1999 11:50:50 AM (Local time)	11
xos.ots	8/31/1999 11:08:50 AM (Local time)	11
soffice.ods	4/16/2009 11:32:48 AM (Local time)	4/
blackberry.ots	10/25/1999 11:52:07 AM (Local time)	11
black_white.ots	10/25/1999 11:51:09 AM (Local time)	11
default.ots	8/24/1999 11:54:50 AM (Local time)	11
diner.ots	8/31/1999 2:15:54 PM (Local time)	11
fall.ots	10/25/1999 11:49:56 AM (Local time)	11
glacier.ots	10/25/1999 11:47:21 AM (Local time)	11
jeans.ots	9/22/1999 4:50:46 PM (Local time)	11
green_grapes.ots	10/25/1999 11:49:36 AM (Local time)	11
nature.ots	10/25/1999 11:45:56 AM (Local time)	11
marine.ots	10/25/1999 11:50:31 AM (Local time)	11

Calc docs
Hangul word processor
Excel
Impress documents
PDF
Powerpoint
Text documents
Word documents
Writer documents

3 - Other Items of Note or Suspicion

`IT-Wks01\Users\james.middleton-adm\NTUSER.DAT:`
`Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`

Extension	Target Name	Value Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	Desktop	10	Desktop.lnk	0	2019-03-28 18:58:42	2019-03-28 18:58:42
RecentDocs	report.html	7	report.lnk	3	2019-03-28 18:56:30	
RecentDocs	D00cihoX0AAFctc.jpg	6	D00cihoX0AAFctc.lnk	4	2019-03-20 22:27:52	
RecentDocs	Database.kdbx	2	Database.kdbx.lnk	5	2019-03-20 22:25:02	
RecentDocs	gmail password.txt	3	gmail password.lnk	7	2019-03-01 17:15:34	
RecentDocs	photo-1522230411790-91c3a622f42e.jfif	4	photo-1522230411790-91c3a622f42e.lnk	8	2019-02-27 19:44:28	
RecentDocs	325462-sdm-vol-1-2abcd-3abcd.pdf	0	325462-sdm-vol-1-2abcd-3abcd.lnk	9	2019-02-27 19:39:53	

`Location C:\Users\noah.beckman\Desktop\OS Final\SOFTWARE: Microsoft\RADAR\HeapLeakDetection`

Target.tmp - Last Dectection Time -2019-02-14 13:29:50
TiWorker.exe
Gadgethost.exe

`Location C:\Users\noah.beckman\Desktop\OS Final\SOFTWARE: Microsoft\Windows\CurrentVersion\Run`

Value Name	Data
beepbep	RegSz "cscript.exe" \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxlQwzP.vbs

Value Name	Value Type	Data
SecurityHealth	RegExpandSz	%ProgramFiles%\Windows Defender\MSASCuiL.exe

Identifiable programs of interest

Timestamp	Key Name	Display Name	Display Version	Install Date	Install Location	Uninstall String
2019-02-14 18:25:09	winscp3_is1	WinSCP 5.13.7	5.13.7	20190214	C:\Program Files (x86)\WinSCP\	"C:\Program Files (x86)\WinSCP\unins000.exe"

C:\Users\noah.beckman\Desktop\OS Final\Users\james.middleton-adm\NTUSER.DAT:
Software\Microsoft\Windows\CurrentVersion\Search\RecentApps
Key Name App Id App Path Last Accessed Launch Count Recent Docs
{9C8214BA-B333-47E3-B803-77C5C15742F4} {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\NOTEPAD.EXE
C:\Windows\system32\notepad.exe 2019-03-01 17:15:34 7 gmail password/C:\Users\james.middleton-adm\Desktop\gmail password.txt: 3/1/2019 5:15:34 PM +00

4 - Local User Accounts

The information below was determined by parsing the registry. Specifically the `SAM\Domains\Account\Users` hive.

IT-WKS01

Username	Enabled	Login Count	Is Admin	Password Expires	Require Password	Locked
Administrator	No	0	Yes	No	Yes	No
Guest	No	0	No	No	Yes	No
Admin	Yes	8	Yes	No	No	No

Username	Creation Time	Last Login	Last Password Change
Administrator	1/26/2019 2:50:28	N/A	N/A
Guest	1/26/2019 2:50:28	N/A	N/A
Admin	1/26/2019 2:54:18	1/28/2019 14:48:23	N/A

PROG-WKS03

Username	Enabled	Login Count	Is Admin	Password Expires	Require Password	Locked
Administrator	No	0	Yes	No	Yes	No
Guest	No	0	No	No	Yes	No
TestLocal	Yes	3	Yes	No	No	No

Username	Creation Time	Last Login	Last Password Change
Administrator	1/26/2019 22:20:00	N/A	N/A
Guest	1/26/2019 22:20:00	N/A	N/A
TestLocal	1/26/2019 23:49:01	1/26/2019 23:53:33	1/26/2019 23:49:01

5 - Remote Desktop Activity

Timestamp	System	Direction	IP Address	User Account	Description
1/25/2019 19:38	it-wks01.E01	Outgoing	192.168.1.254	james.middleton-adm	A logon was attempted using explicit credentials.
1/25/2019 19:38	it-wks01.E01	Outgoing	192.168.1.254	james.middleton-adm	A logon was attempted using explicit credentials.
1/25/2019 19:38	it-wks01.E01	Outgoing		james.middleton-adm	A logon was attempted using explicit credentials.
1/25/2019 19:38	it-wks01.E01	Outgoing	192.168.1.254	james.middleton-adm	A logon was attempted using explicit credentials.
1/25/2019 19:38	it-wks01.E01	Outgoing		james.middleton-adm	A logon was attempted using explicit credentials.

1/25/2019 19:38	it-wks01.E01	Outgoing	192.168.1.254	james.middleton-adm	A logon was attempted using explicit credentials.
1/25/2019 19:38	it-wks01.E01	Outgoing		james.middleton-adm	A logon was attempted using explicit credentials.
1/25/2019 19:38	it-wks01.E01	Outgoing		james.middleton-adm	A logon was attempted using explicit credentials.
1/25/2019 19:39	it-wks01.E01	Outgoing		james.middleton-adm	A logon was attempted using explicit credentials.
1/25/2019 19:39	it-wks01.E01	Outgoing		james.middleton-adm	A logon was attempted using explicit credentials.
1/26/2019 18:55	prog-wks03.E01	Outgoing		roger.melton	A logon was attempted using explicit credentials.
1/26/2019 18:55	prog-wks03.E01	Outgoing	192.168.1.254	roger.melton	A logon was attempted using explicit credentials.
1/26/2019 18:55	prog-wks03.E01	Outgoing		roger.melton	A logon was attempted using explicit credentials.
1/26/2019 18:55	prog-wks03.E01	Outgoing	192.168.1.254	roger.melton	A logon was attempted using explicit credentials.
2/23/2019 13:32	it-wks01.E01	Outgoing	192.168.3.103		
2/23/2019 13:47	it-wks01.E01	Outgoing	192.168.3.103		
2/23/2019 13:58	it-wks01.E01	Outgoing	192.168.3.103		
2/23/2019 13:58	it-wks01.E01	Outgoing	192.168.3.103		
2/23/2019 14:06	it-wks01.E01	Outgoing	192.168.3.103		
2/23/2019 14:08	it-wks01.E01	Incoming	192.168.3.103	james.middleton-adm	
2/23/2019 14:08	it-wks01.E01	Incoming	192.168.3.103	GRRU\james.middleton-adm	

2/23/2019 14:08	it-wks01.E01	Incoming	192.168.3.103	GRRU\james.middleton-adm	Remote Desktop Services: Session has been disconnected.
3/28/2019 14:35	prog-wks03.E01	Incoming	192.168.1.254	james.middleton-adm	
3/28/2019 14:35	prog-wks03.E01	Incoming	192.168.1.254	PROG-WKS03$	An account was successfully logged on.
3/28/2019 14:35	prog-wks03.E01	Incoming	192.168.1.254	PROG-WKS03$	An account was successfully logged on.
3/28/2019 14:36	prog-wks03.E01	Incoming	192.168.1.254	GRRU\james.middleton-adm	Remote Desktop Services: Session logon succeeded.
3/28/2019 14:36	prog-wks03.E01	Incoming	192.168.1.254	GRRU\james.middleton-adm	Remote Desktop Services: Shell start notification received.
3/28/2019 14:47	prog-wks03.E01	Incoming	192.168.1.254	GRRU\james.middleton-adm	Remote Desktop Services: Session has been disconnected.
3/28/2019 14:55	it-wks01.E01	Incoming	192.168.1.254	james.middleton-adm	
3/28/2019 14:55	it-wks01.E01	Incoming	192.168.1.254	GRRU\james.middleton-adm	
3/28/2019 15:03	it-wks01.E01	Incoming	192.168.1.254	GRRU\james.middleton-adm	Remote Desktop Services: Session has been disconnected.
3/28/2019 17:35	prog-wks03.E01	Incoming	192.168.1.254	GRRU\james.middleton-adm	
3/28/2019 17:35	prog-wks03.E01	Incoming	192.168.1.254	james.middleton-adm	
3/28/2019 18:30	prog-wks03.E01	Incoming	192.168.1.254	GRRU\james.middleton-adm	Remote Desktop Services: Session has been disconnected.