

# Windows IR Live Forensics Cheat Sheet by [koriley](#)

Based on John Strand's Webcast - Live Windows Forensics..

[first](#)[windows](#)[forensics](#)[ir](#)[responder](#)

## Unusual Network Usage

## Unusual Processes

### Task List

tasklist

`wmic process list full'

### Parend Process ID

wmic process get name,parentprocessid,  
processid

### Command-Line Options and DLLs

tasklist /m /fi "pid eq [pid]"

wmic process where processid=[pid] get  
commandline

### Run Task Manager: Start->Run... and type taskmgr.exe

- Look for unusual/unexpected processes

Look at File Shares	<code>net view \\127.0.0.1</code>
Open Sessions with Machine	<code>net session</code>
Session This machine has Opened	<code>net use</code>
NetBIOS over TCP/IP Activity	<code>nbtstat -S</code>
List Listening TCP and UDP Ports	<code>netstat -na</code>
5 - Continuous Scrolling every 5 seconds	<code>netstat -na 5</code>
-o flag shows process ID -b flag shows executable	<code>netstat -naob</code>
Inspect Firewall rules	<code>netsh advfirewall show currentprofile</code>
	<code>netsh firewall show config</code>

Unusual Accounts	
Unexpected Users in the Administrators Group	<code>lusrmgr.msc</code>
List Users	<code>net user</code>
List Members of Admin Group	<code>net localgroup administrators</code>
List Domain Users	<code>net user /domain</code>
When looking at domain accounts, the command will be run on the domain controller. A large domain may take some time - redirect to a text file to analyze: <code>net user /domain &gt; domainUsers.txt</code>	

- Focus on processes with username **SYSTEM** or **ADMINISTRATOR** or user in the **Local Administrator's** group.

Unusual Scheduled Tasks	
List System Scheduled Tasks	<code>schtasks</code>
You can also use the Task Scheduler GUI: <b>Start-&gt;Programs-&gt;Accessories-&gt;System Tools-&gt;Scheduled Tasks</b>  Look for unusual Tasks run as a user of the Local Admin, SYSTEM, or blank username	

### Windows Security & System Events To Look For

Security 4720	User Account Created
Security 4722	User Account Enabled
Security 4724	Password Reset
Security 4738	User Account Change
Security 4732	Account Added or Removed From Group
Security 1102	Audit Log Cleared
System 7030	Basic Service Operations
System 7045	Service Was Installed
System 1056	DHCP Server Oddities
System 10000	COM Functionality
System 20001	Device Driver Installation
System 20002	Remote Access
System 20003	Service Installation

### Search for Other Startup Items

Users' Autostart Folders	<pre>dir /s /b "C:\Documents and Settings\ [user name]\Start Menu\"</pre> <pre>dir /s /b "C:\Users\ [user name]\Start Menu\"</pre>
Use WMIC To find Start Up Programs	<pre>wmic startup list full</pre>

### Unusual Reg Key Entries

**Check the Registry Run keys for malware that has made an entry to launch itself.**

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunonceEx

```
C:\>reg query hklm\software\microsoft\windows\currentversion\run
```

These can also be analyzed with `regedit.exe`.

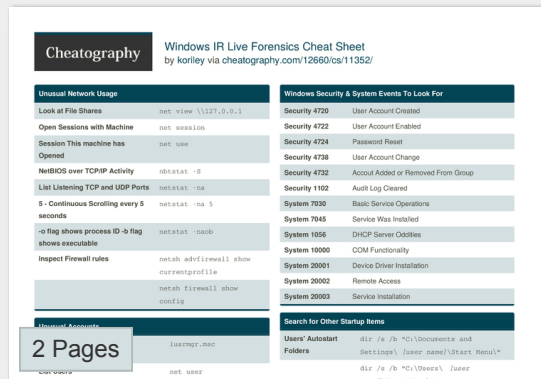
`Autoruns.exe` from **Sysinternals** will pull all **Auto Start Entry Points**.

### Unusual Services

Services Control Panel	<code>services.msc</code>
List Of Services Available	<code>net start</code>
Show Service Detail	<code>sc query   more</code>
Map of Service from Which Process	<code>tasklist /svc</code>

# Download the Windows IR Live Forensics Cheat Sheet

# Share This Cheat Sheet!



PDF (recommended)

 [PDF \(2 pages\)](#)

Alternative Downloads

 [PDF \(black and white\)](#)

 [LaTeX](#)



## Comments

No comments yet. Add yours below!

## Add a Comment

Your Comment



Your Name

## Cheatographer



## Metadata

Languages: [English](#)



Your Email Address

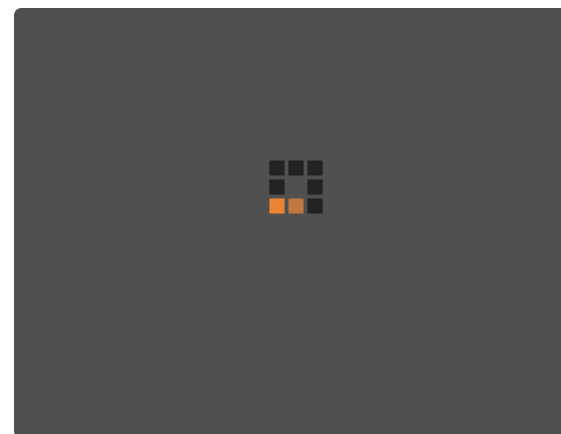
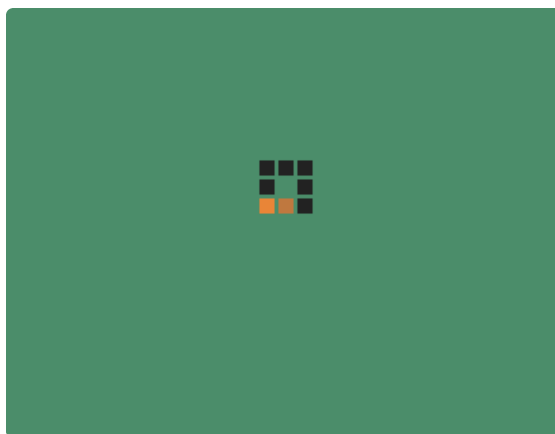
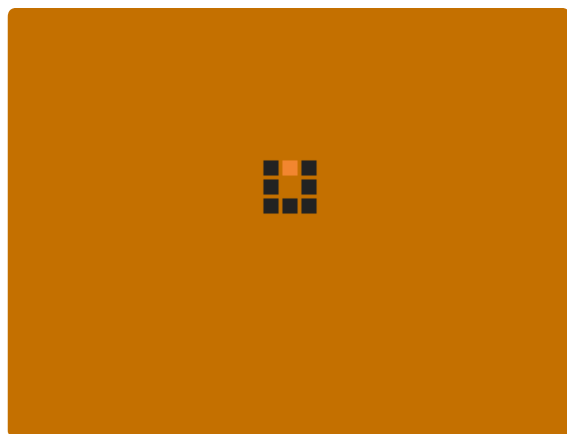


Your Comment

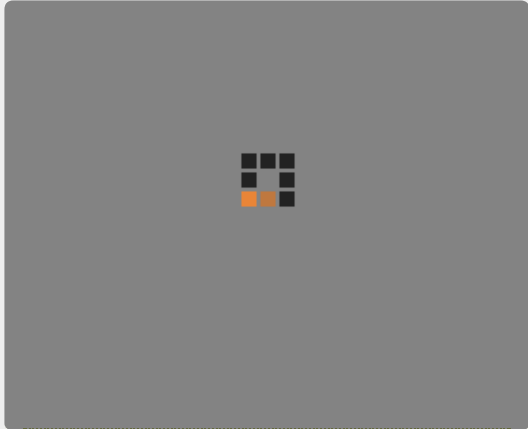
Post Your Comment

Published: 4th April, 2017

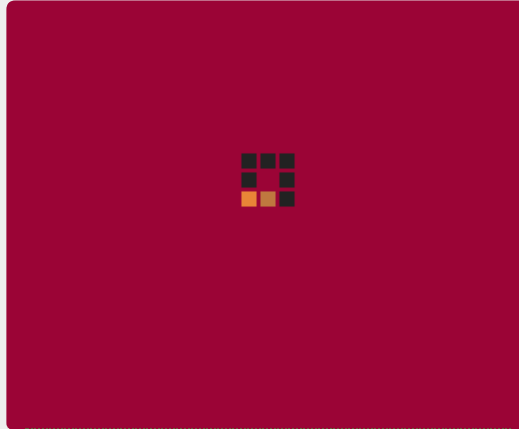
## Related Cheat Sheets



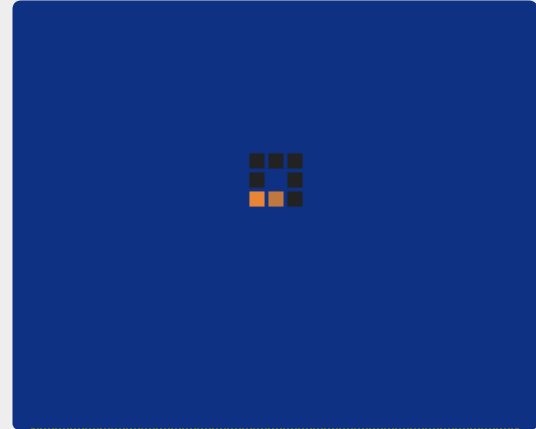
## Latest Cheat Sheet



## Most Popular Cheat Sheet



## Random Cheat Sheet



## About Cheatography

Cheatography is a collection of 4067 cheat sheets and quick references in 25 languages for everything from history to travel!

## On The Blog


*10th June*

### 5 Ways Cheatography Benefits Your Business

Cheatography Cheat Sheets are a great timesaver for individuals - coders, gardeners, musicians, everybody! But businesses can benefit from them as well - read on to find out more.

## Recent Activity

 williamcollins published NTLK Language Processing Python.  
5 hours 13 mins ago

 seannarr published Draft - Rust Book Notes - Not a.  
9 hours 33 mins ago

ShotCare updated Oregon Immunization.  
11 hours 14 mins ago

## Behind the Scenes

## Cheatography RSS Feeds

 Latest Cheat Sheets

## Share Cheatography!



If you have any problems, or just want to say hi,  
you can find us right here:

 [Latest Blog Posts](#)



[DaveChild](#)



[SpaceDuck](#)



[Cheatography](#)

---

© 2011 - 2018 Cheatography.com | [CC License](#) | [Terms](#) | [Privacy](#)

Site by [Get. Post. Cookie.](#)