# RegEx Cheat Sheet

## Anchors

| | |
|---|---|
| ^ | Start of line |
| **\A** | Start of string |
| **$** | End of line |
| **\Z** | End of string |
| **\b** | Word boundary |
| **\B** | Not word boundary |
| \< | Start of word |
| \> | End of word |

## Character Classes

| | |
|---|---|
| **\c** | Control character |
| **\s** | White space |
| **\S** | Not white space |
| **\d** | Digit |
| **\D** | Not digit |
| **\w** | Word |
| **\W** | Not word |
| **\xhh** | Hex character |

## Quantifiers

| | |
|---|---|
| * | 0 or more |
| + | 1 or more |
| ? | 0 or 1 |
| {3} | Exactly 3 |
| {3,} | 3 or more |
| {3,5} | 3, 4, or 5 + |

## Pattern Modifiers

| | |
|---|---|
| **g** | Global match |
| **i** | Case insensitive |
| **s** | String as single line |
| **m** | Multiple lines |
| **U** | Ungreedy pattern |

## Special Characters

| | |
|---|---|
| \ | Escape character |
| **\n** | New line |
| **\r** | Carriage return |
| **\r** | Tab |
| **\v** | Vertical tab |
| **\f** | Form feed |
| **\a** | Alarm |
| **[\b]** | Backspace |
| **\e** | Escape |

## Ranges

| | |
|---|---|
| **.** | Any character except new line |
| **(a\|b)** | a or b |
| **(…)** | Group |
| **(?:…)** | Passive Group |
| **[^abc]** | Not a or b or c |
| **[a-q]** | Lowercase letter between a and q |
| **[A-Q]** | Uppercase letter between A and Q |
| **[0-7]** | Digit between 0 and 7 |

## Assertions

| | |
|---|---|
| **(?=)** | Lookahead assertion |
| **(?!)** | Negative lookahead |
| **(?<=)** | Lookbehind assertion |
| **(?!=) or (?<!)** | Negative Lookbehind |
| **(?())** | If Then Condition |
| **(?()\|)** | If Then Else Condition |
| **(?#)** | Comment |

| | |
|---|---|
| **Metacharacters (Escape These!)** | **. * + ? ^ $ [ () { . ** |

AND
APPLIED NETWORK DEFENSE

http://networkdefense.io - http://regextraining.com

# Common DFIR RegEx

## Common Hash Formats

<table>
<tr><td><b>MD5</b></td><td>[a-fA-F0-9]{32}</td><td><b>SHA256</b></td><td>[a-fA-F0-9]{64}</td></tr>
<tr><td><b>SHA1</b></td><td>[a-fA-F0-9]{40}</td><td><b>SHA512</b></td><td>[a-fA-F0-9]{128}</td></tr>
</table>

## IP Addresses

<table>
<tr><td><b>IPv4 (Simple)</b></td><td>(?:\d{1,3}\.){3}\d{1,3}</td></tr>
<tr><td><b>IPv4 (Accurate)</b></td><td>(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)</td></tr>
<tr><td><b>IPv6</b></td><td>(?:[a-fA-F0-9]{1,4}:){7}[a-fA-F0-9]{1,4}</td></tr>
</table>

## MAC Address

<table>
<tr><td><b>MAC</b></td><td>[0-9A-F]{2}([-:]?)(?:[0-9A-F]{2}\1){4}[0-9A-F]{2}</td></tr>
</table>

## Encoding / Data Format

<table>
<tr><td><b>Base64</b></td><td>^(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=)?$</td></tr>
<tr><td><b>Hex</b></td><td>/^#?([a-f0-9]{6}|[a-f0-9]{3})$/</td></tr>
</table>

## E-Mail

<table>
<tr><td><b>Address</b></td><td>/^([a-z0-9_\.-]+)@([\da-z\.-]+)\.([a-z\.]{2,6})$/</td></tr>
</table>

## URLs

<table>
<tr><td><b>Constituent parts of HTTP/HTTPS URL - Insensitive inline modifier</b></td><td>(?i)(?<URL>(?<scheme>https?)://(?<domain>[^/:]+(?<=\.(?<TLD>[^/:]+)))(?(?=:):(?<port>\d{1,5})|)(?(?=/)(?<URI>/[^/]+)+(?<file>/[^.]+\.\S+)?))</td></tr>
<tr><td><b>Constituent parts of HTTP/HTTPS URL - No modifier</b></td><td>(<URL>(?<scheme>[hH][tT]{2}[pP][sS]?)://(?<domain>[^/:]+(?<=\.(?<TLD>[^/:]+)))(?(?=:):(?<port>\d{1,5})|)(?(?=/)(?<URI>/[^/]+)+(?<file>/[^.]+\.\S+)?))</td></tr>
</table>

## Directory/File Path

<table>
<tr><td><b>Drive</b></td><td>(?x)(?>\b[a-z]:|\\\\[a-z0-9 %._~-]{1,63}\\[a-z0-9 $%._~-]{1,80})\\</td></tr>
<tr><td><b>Folder</b></td><td>(?>[^\\/:*?"<>|\x00-\x1F]{0,254}[^.\\/:*?"<>|\x00-\x1F]\\)*</td></tr>
<tr><td><b>File</b></td><td>(?>[^\\/:*?"<>|\x00-\x1F]{0,254}[^.\\/:*?"<>|\x00-\x1F])?</td></tr>
<tr><td><b>Standard Path</b></td><td>(?>\b[a-z]:|\\\\[a-z0-9 %._~-]{1,63}\\[a-z0-9 $%._~-]{1,80})\\(?>[^\\/:*?"<>|\x00-\x1F]{0,254}[^.\\/:*?"<>|\x00-\x1F]\\)*(?>[^\\/:*?"<>|\x00-\x1F]{0,254}[^.\\/:*?"<>|\x00-\x1F])?</td></tr>
<tr><td><b>Windows Path</b></td><td>[a-z]:\\(?>[^\\/:*?"<>|\x00-\x1F]{0,254}[^.\\/:*?"<>|\x00-\x1F]\\)*(?>[^\\/:*?"<>|\x00-\x1F]{0,254}[^.\\/:*?"<>|\x00-\x1F])?</td></tr>
</table>

AND
APPLIED NETWORK DEFENSE

http://networkdefense.io - http://regextraining.com