```
{
  "took" : 7,
  "timed_out" : false,
  "_shards" : {
    "total" : 10,
    "successful" : 10,
    "failed" : 0
  },
  "hits" : {
    "total" : 142401,
    "max_score" : 1.0,
    "hits" : [ {
      "_index" : "topbeat-2016.04.16",
      "_type" : "process",
      "_id" : "AVQgGgXE6PGR8o53cT-4",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2016-04-16T17:20:31.210Z",
        "beat" : {
          "hostname" : "DESKTOP-4E45CI8",
          "name" : "DESKTOP-4E45CI8"
        },
        "count" : 1,
        "proc" : {
          "cmdline" : "igfxTray.exe ",
          "cpu" : {
            "user" : 93,
            "user_p" : 0,
            "system" : 234,
            "total" : 327,
            "start_time" : "Sep26"
          },
          "mem" : {
            "size" : 3407872,
            "rss" : 11038720,
            "rss_p" : 0,
            "share" : 0
          },
          "name" : "igfxTray.exe",
          "pid" : 3824,
          "ppid" : 0,
          "state" : "running",
          "username" : "DESKTOP-4E45CI8\\user"
        },
        "type" : "process"
      }
    }, {
      "_index" : "topbeat-2016.04.16",
      "_type" : "process",
      "_id" : "AVQgGgYE6PGR8o53cT-8",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2016-04-16T17:20:31.234Z",
        "beat" : {
          "hostname" : "DESKTOP-4E45CI8",
          "name" : "DESKTOP-4E45CI8"
        },
        "count" : 1,
        "proc" : {
          "cmdline" : "\"C:\\Program Files\\Conexant\\MicTray\\MicTray64.exe\" ",
          "cpu" : {
            "user" : 453,
            "user_p" : 0,
            "system" : 406,
            "total" : 859,
            "start_time" : "Sep26"
          },
          "mem" : {
            "size" : 2170880,
            "rss" : 9670656,
            "rss_p" : 0,
            "share" : 0
          },
          "name" : "MicTray64.exe",
          "pid" : 4120,
          "ppid" : 0,
          "state" : "running",
          "username" : "DESKTOP-4E45CI8\\user"
        },
        "type" : "process"
      }
    }, {
      "_index" : "topbeat-2016.04.16",
      "_type" : "process",
      "_id" : "AVQgGgYE6PGR8o53cT--",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2016-04-16T17:20:31.246Z",
        "beat" : {
          "hostname" : "DESKTOP-4E45CI8",
          "name" : "DESKTOP-4E45CI8"
        },
        "count" : 1,
        "proc" : {
          "cmdline" : "\"C:\\Program Files\\AMD\\CNext\\CNext\\RadeonSettings.exe\"
atlogon",
          "cpu" : {
            "user" : 2562,
            "user_p" : 0,
            "system" : 1250,
            "total" : 3812,
            "start_time" : "Sep26"
          },
          "mem" : {
            "size" : 102445056,
            "rss" : 24064000,
            "rss_p" : 0,
            "share" : 0
          },
          "name" : "RadeonSettings.exe",
          "pid" : 3240,
          "ppid" : 0,
          "state" : "running",
          "username" : "DESKTOP-4E45CI8\\user"
        },
        "type" : "process"
      }
    }, {
      "_index" : "topbeat-2016.04.16",
      "_type" : "process",
      "_id" : "AVQgGgYE6PGR8o53cT_C",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2016-04-16T17:20:31.274Z",
        "beat" : {
          "hostname" : "DESKTOP-4E45CI8",
          "name" : "DESKTOP-4E45CI8"
        },
        "count" : 1,
          "proc" : {
            "cmdline" : "\"C:\\Program Files (x86)\\Common Files\\Java\\Java
  Update\\jusched.exe\" ",
            "cpu" : {
              "user" : 15,
              "user_p" : 0,
              "system" : 31,
              "total" : 46,
              "start_time" : "Sep26"
            },
            "mem" : {
              "size" : 1855488,
              "rss" : 11300864,
              "rss_p" : 0,
              "share" : 0
            },
            "name" : "jusched.exe",
            "pid" : 4136,
            "ppid" : 0,
            "state" : "running",
            "username" : "DESKTOP-4E45CI8\\user"
          },
          "type" : "process"
        }
      }, {
        "_index" : "topbeat-2016.04.16",
        "_type" : "process",
        "_id" : "AVQgGgYE6PGR8o53cT_D",
        "_score" : 1.0,
        "_source" : {
          "@timestamp" : "2016-04-16T17:20:31.284Z",
          "beat" : {
            "hostname" : "DESKTOP-4E45CI8",
            "name" : "DESKTOP-4E45CI8"
          },
          "count" : 1,
          "proc" : {
            "cmdline" : "\"C:\\Program Files (x86)\\Hewlett-Packard\\Shared\\hpqwmiex.exe\"",
            "cpu" : {
              "user" : 515,
              "user_p" : 0,
              "system" : 140,
              "total" : 655,
              "start_time" : "Sep26"
            },
            "mem" : {
              "size" : 1818624,
              "rss" : 8548352,
              "rss_p" : 0,
              "share" : 0
            },
            "name" : "hpqwmiex.exe",
            "pid" : 3208,
            "ppid" : 0,
            "state" : "running",
            "username" : "NT AUTHORITY\\SYSTEM"
          },
          "type" : "process"
        }
      }, {
        "_index" : "topbeat-2016.04.16",
        "_type" : "process",
        "_id" : "AVQgGgYE6PGR8o53cT_F",
        "_score" : 1.0,
        "_source" : {
          "@timestamp" : "2016-04-16T17:20:31.305Z",
          "beat" : {
            "hostname" : "DESKTOP-4E45CI8",
            "name" : "DESKTOP-4E45CI8"
          },
          "count" : 1,
          "proc" : {
            "cmdline" : "C:\\Windows\\system32\\wbem\\unsecapp.exe -Embedding",
            "cpu" : {
              "user" : 0,
              "user_p" : 0,
              "system" : 46,
              "total" : 46,
              "start_time" : "Sep26"
            },
            "mem" : {
              "size" : 1220608,
              "rss" : 6701056,
              "rss_p" : 0,
              "share" : 0
            },
            "name" : "unsecapp.exe",
            "pid" : 1476,
            "ppid" : 0,
            "state" : "running",
            "username" : "DESKTOP-4E45CI8\\user"
          },
          "type" : "process"
        }
      }, {
        "_index" : "topbeat-2016.04.16",
        "_type" : "process",
        "_id" : "AVQgGgYE6PGR8o53cT_O",
        "_score" : 1.0,
        "_source" : {
          "@timestamp" : "2016-04-16T17:20:31.404Z",
          "beat" : {
            "hostname" : "DESKTOP-4E45CI8",
            "name" : "DESKTOP-4E45CI8"
          },
          "count" : 1,
          "proc" : {
            "cmdline" : "C:\\Windows\\System32\\InstallAgent.exe -Embedding",
            "cpu" : {
              "user" : 62,
              "user_p" : 0,
              "system" : 15,
              "total" : 77,
              "start_time" : "Sep26"
            },
            "mem" : {
              "size" : 2260992,
              "rss" : 13189120,
              "rss_p" : 0,
              "share" : 0
            },
            "name" : "InstallAgent.exe",
            "pid" : 5704,
            "ppid" : 0,
            "state" : "running",
            "username" : "DESKTOP-4E45CI8\\user"
          },
          "type" : "process"
        }
      }, {
```

```
      "_index" : "topbeat-2016.04.16",
      "_type" : "process",
      "_id" : "AVQgGgYE6PGR8o53cT_S",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2016-04-16T17:20:31.449Z",
        "beat" : {
          "hostname" : "DESKTOP-4E45CI8",
          "name" : "DESKTOP-4E45CI8"
        },
        "count" : 1,
        "proc" : {
          "cmdline" : "\"C:\\Program Files (x86)\\Google\\Chrome\\Application\\chrome.exe\"
--type=crashpad-handler /prefetch:7 --no-rate-limit \"--
database=C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\Crashpad\" --
url=https://clients2.google.com/cr/report --annotation=channel=m --annotation=plat=Win32 --
annotation=prod=Chrome --annotation=ver=50.0.2661.75 --handshake-handle=0x1ac",
          "cpu" : {
            "user" : 31,
            "user_p" : 0,
            "system" : 15,
            "total" : 46,
            "start_time" : "Sep26"
          },
          "mem" : {
            "size" : 1638400,
            "rss" : 6221824,
            "rss_p" : 0,
            "share" : 0
          },
          "name" : "chrome.exe",
          "pid" : 6424,
          "ppid" : 0,
          "state" : "running",
          "username" : "DESKTOP-4E45CI8\\user"
        },
        "type" : "process"
      }
    }, {
      "_index" : "topbeat-2016.04.16",
      "_type" : "process",
      "_id" : "AVQgGgYE6PGR8o53cT_V",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2016-04-16T17:20:31.482Z",
        "beat" : {
          "hostname" : "DESKTOP-4E45CI8",
          "name" : "DESKTOP-4E45CI8"
        },
        "count" : 1,
        "proc" : {
          "cmdline" : "\"C:\\Program Files (x86)\\Google\\Chrome\\Application\\chrome.exe\"
--type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,WebFontsIntervention<WebFontsInterve
ntion --disable-features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup --
lang=en-US --force-
fieldtrials=AppBannerTriggering/Aggressive/AutofillProfileOrderByFrecency/Enabled/*Automati
cTabDiscarding/Enabled_Once_10-
gen2/BrotliEncoding/Default/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disable
d/*ClientSideDetectionModel/Model0/*CrossDevicePromo/1DaySingleProfile/*DataReductionProxyC
onfigService/Enabled/*DirectWriteFontProxy/UseDirectWriteFontProxy/*ExtensionActionRedesign
/Enabled/ExtensionDeveloperModeWarning/Enabled/*ExtensionInstallVerification/Enforce/*GFE/D
efault/InstanceID/Enabled/MaterialDesignDownloads/Enabled/*NetworkQualityEstimator/Enabled/
*OmniboxBundledExperimentV1/PP_Ethersuggest_A6_Stable_R8/PasswordBranding/Disabled/*Passwor
dGeneration/Disabled/*PreRead/Default/*QUIC/EnabledNoId/ReportCertificateErrors/ShowAndPoss
```

```
iblySend/*ResourcePriorities/Control50pct/SHA1IdentityUIWarning/Enabled/SHA1ToolbarUIJanuar
y2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTPromptFieldTrial/On/SSLCommonNameMismatchH
andling/Disabled/*SafeBrowsingIncidentReportingService/Default/SafeBrowsingIncidentReportin
gServiceFeatures/Default/SafeBrowsingUnverifiedDownloads/DisableByParameterMostSbTypes2/Saf
eBrowsingUpdateFrequency/Default/*TriggeredResetFieldTrial/On/*UMA-Dynamic-Uniformity-
Trial/Group3/*UMA-Population-Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_20/*UMA-
Uniformity-Trial-10-Percent/default/*UMA-Uniformity-Trial-100-Percent/group_01/*UMA-
Uniformity-Trial-20-Percent/group_04/*UMA-Uniformity-Trial-5-Percent/group_02/*UMA-
Uniformity-Trial-50-
Percent/group_01/*UseDelayAgnosticAEC/DefaultEnabled/*WebFontsIntervention/Enabled/WebRTC-
LocalIPPermissionCheck/Enabled/WebRTC-PeerConnectionDTLS1.2/Enabled/ --enable-offline-auto-
reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --
num-raster-threads=2 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553 --video-image-
texture-target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553 --
channel=\"6372.4.1926229429\\266482366\" /prefetch:1",
          "cpu" : {
            "user" : 96578,
            "user_p" : 0.0115,
            "system" : 4765,
            "total" : 101343,
            "start_time" : "Sep26"
          },
          "mem" : {
            "size" : 72732672,
            "rss" : 83075072,
            "rss_p" : 0.01,
            "share" : 0
          },
          "name" : "chrome.exe",
          "pid" : 7028,
          "ppid" : 0,
          "state" : "running",
          "username" : "DESKTOP-4E45CI8\\user"
        },
        "type" : "process"
      }
    }, {
      "_index" : "topbeat-2016.04.16",
      "_type" : "process",
      "_id" : "AVQgGgYE6PGR8o53cT_b",
      "_score" : 1.0,
      "_source" : {
        "@timestamp" : "2016-04-16T17:20:31.543Z",
        "beat" : {
          "hostname" : "DESKTOP-4E45CI8",
          "name" : "DESKTOP-4E45CI8"
        },
        "count" : 1,
        "proc" : {
          "cmdline" : "\"C:\\Program Files (x86)\\Google\\Chrome\\Application\\chrome.exe\"
--type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,WebFontsIntervention<WebFontsInterve
ntion --disable-features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup --
lang=en-US --force-
fieldtrials=AppBannerTriggering/Aggressive/AutofillProfileOrderByFrecency/Enabled/*Automati
cTabDiscarding/Enabled_Once_10-
gen2/BrotliEncoding/Default/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disable
d/*ClientSideDetectionModel/Model0/*CrossDevicePromo/1DaySingleProfile/*DataReductionProxyC
onfigService/Enabled/*DirectWriteFontProxy/UseDirectWriteFontProxy/*ExtensionActionRedesign
/Enabled/ExtensionDeveloperModeWarning/Enabled/*ExtensionInstallVerification/Enforce/*GFE/D
efault/InstanceID/Enabled/MaterialDesignDownloads/Enabled/*NetworkQualityEstimator/Enabled/
*OmniboxBundledExperimentV1/PP_Ethersuggest_A6_Stable_R8/PasswordBranding/Disabled/*Passwor
dGeneration/Disabled/*PreRead/Default/*QUIC/EnabledNoId/ReportCertificateErrors/ShowAndPoss
iblySend/*ResourcePriorities/Control50pct/SHA1IdentityUIWarning/Enabled/SHA1ToolbarUIJanuar
```

```
y2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTPromptFieldTrial/On/SSLCommonNameMismatchH
andling/Disabled/*SafeBrowsingIncidentReportingService/Default/SafeBrowsingIncidentReportin
gServiceFeatures/Default/SafeBrowsingUnverifiedDownloads/DisableByParameterMostSbTypes2/*Sa
feBrowsingUpdateFrequency/Default/*TriggeredResetFieldTrial/On/*UMA-Dynamic-Uniformity-
Trial/Group3/*UMA-Population-Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_20/*UMA-
Uniformity-Trial-10-Percent/default/*UMA-Uniformity-Trial-100-Percent/group_01/*UMA-
Uniformity-Trial-20-Percent/group_04/*UMA-Uniformity-Trial-5-Percent/group_02/*UMA-
Uniformity-Trial-50-
Percent/group_01/*UseDelayAgnosticAEC/DefaultEnabled/*WebFontsIntervention/Enabled/WebRTC-
LocalIPPermissionCheck/Enabled/WebRTC-PeerConnectionDTLS1.2/Enabled/ --enable-offline-auto-
reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --
num-raster-threads=2 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553 --video-image-
texture-target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553 --
channel=\"6372.7.2120320291\\1970729016\" /prefetch:1",
          "cpu" : {
            "user" : 109640,
            "user_p" : 0.0136,
            "system" : 10312,
            "total" : 119952,
            "start_time" : "Sep26"
          },
          "mem" : {
            "size" : 71680000,
            "rss" : 80072704,
            "rss_p" : 0.01,
            "share" : 0
          },
          "name" : "chrome.exe",
          "pid" : 6168,
          "ppid" : 0,
          "state" : "running",
          "username" : "DESKTOP-4E45CI8\\user"
        },
        "type" : "process"
      }
    } ]
  }
}
```