Foundstone's *Riffle* Forensic Artifact Collection Tool
Frequently Asked Questions

1. **What is *Riffle*?**
   Riffle is a highly configurable Win32 console application that collects forensic artifacts from a live Windows system. These artifacts are then placed in a Foundstone malware correlation database and examined for indicators of compromise (IOC's).

2. **How does it work?**
   The tool consists of two files, the command executable and a standard INI file used to configure the actions the tool performs. Both files are placed on a Windows host and the application is run under the local administrator or system privilege level.

   The tool extracts the requested artifacts and places them into a 7Zip compressed archive file. This file can be left on the host filesystem for later retrieval, or delivered to another location via FTP, a Windows SMB share, or even E-Mailed if it is less than 5MB in size.

3. **Why do we need another forensic tool?**
   Foundstone incident response consultants have responded to hundreds of high profile security compromise incidents over the last few years. Identifying hosts compromised by malware and searching for IOC's in large environments is always a challenge. There are many free, open-source, and expensive third-party tools that can assist in this task. The one common downside of these tools is their complexity and intrusive nature.

   The Foundstone IR team decided to build a forensic artifact collection tool that is lightweight, flexible, easy to deploy, scalable, and effective at finding compromised computers. In fact, *riffle* is really a combination of tools since it uses some of the best free and open-source system utilities available anywhere.

4. **Why kind of artifacts does *Riffle* collect?**
   Since riffle is a forensic tool, the artifacts it collects are those that are most valuable to forensic investigators. The real power of *Riffle* is its ability to collect artifacts from a live Windows system that are not easily obtainable because they are locked by the operating system. This includes the $MFT, event logs, registry hives, NTUser.dat files, etc. Riffle is quite versatile. It will collect as many or as few artifacts as you desire. The settings in the riffle.ini file determine what actions it takes.

   Below is a list of the tasks *Riffle* can perform:

   - Extracts a live $MFT using sector-level disk reads.
   - Extract the Registry hives (SYSTEM, SECURITY, APPLICATION, and SAM)
   - Extract Windows event logs.
   - Extracts the contents of the Windows Prefetch folder on workstations.
   - Extract NTUser.dat files of all user profiles.
   - Executes *at* and *schtasks* and saves output to determine scheduled tasks.
   - Executes *netstat –ano* and saves output to determine network connections.
   - Executes *tasklist -fo csv -v* to determine running processes with PID's.
   - Executes *tasklist -fo csv /svc* to determine what services are running under a task.
   - Executes *ipconfig /displaydns* and saves output to determine DNS activity.
   - Executes *ipconfig* and saves output to determine network configuration
   - Extracts the contents of the hosts file.
   - Extracts McAfee A/V log files including On-Access and Access Protection logs.
   - Extracts contents of McAfee A/V Quarantine folder.
   - Extract Internet history from Internet Explorer and FireFox.

In addition, *Riffle* carries within its own payload, useful tools to do additional artifact collection. This includes:

- SysInternals® *PSLogList* is used to extract live event logs including the conversion of the logs to a csv file containing textual context of the events obtained from the host.*
- SysInternals® *Autorunsc* console tool is used to identify start-up applications, services and drivers. This versatile tool also hashes all of the startup binaries it detects.*
- *md5deep* is used to hash files on the %SYSTEMDRIVE%. This proven workhorse is a very efficient and powerful hashing tool. If hashing is enabled in the INI file, by default, *Riffle* will hash all files in the user profile folder (Documents and Settings, or Users) and the entire Window folder. You can also hash all the files on the system volume if desired.

5. **How long does *Riffle* take to collect these artifacts?**

   There are a few variables here, but in general, Riffle takes less than five minutes to complete its tasks. If you enable hashing, it could take considerably longer. Remember, *Rifflle* was designed to be lightweight and efficient. There is no installer, no agent, no server. You place the tool on a host and run it once. It's that simple.

6. **What do you do with the artifacts *Riffle* collects?**

   The collected artifacts are securely transported or transmitted to the Foundstone forensic lab for analysis. The data is collated and placed in an optimized database for analysis. The data is then analyzed by experienced forensic analysts highly trained in identifying indicators of IOC's. In classified or other highly secure facilities, this analysis can be done on-site if required.

7. **What happens if you identify compromised computers?**

   During IOC analysis, if a host is believed to be compromised, the client is immediately notified so containment and remediation decisions can be made as quickly as possible. Depending on the seriousness of the compromise, Foundstone will provide emergency incident response investigators to assist in this effort.

8. **What if I have a large number of computers I want you to analyze?**

   Due to the lightweight nature of *Riffle*, the tool can be deployed to thousands of hosts. Within minutes the forensic artifact archives collected from these hosts can be delivered to a centralized location for submission to the forensic lab.

9. **How do I know the data you collect will be handled in a secure and confidential manner?**

   Security is Foundstone's only business. Our entire malware assessment service practice is built around protecting you and your data. The *Riffle* artifact archive can be encrypted with a single switch in the INI file. In fact, the INI file can also be encrypted. From the time your data is collected until it is securely deleted off our malware correlation servers after analysis, it is always maintained in a highly secure environment.

10. **Who do I contact if I want to learn more about Foundstone's malware assessment services?**

    Foundstone is ready to help you solve your digital security challenges.
    You can call us at **877-913-6863**.
    You can also send us an email – consulting@foundstone.com.