**FastIR-Logstash-Flask Example**

Intrusion Detection can be done by 2 types of analysis: Signature Analysis and Protocol Analysis.

Signature Analysis is when a particular malware is not new and its hash has been made public. By comparing the hash of a file believed to be malware with the database of hashes of known malwares, it can thus be identified if any file in the system is malicious.

Protocol Analysis is when network traffic is monitored and analysed, looking out for anomalies in the network traffic and deviations from the protocol that may be indicative of a compromise.

Horangi uses FastIR, which collects the most essential live Windows Artefacts quickly and analyses it to ensure that there are no malicious files in the system.

After data is collected by FastIR, the file is parsed by csv2es.py to Elasticsearch, a search engine that allows powerful queries.

The artefacts chosen to be stored on Elasticsearch are:

* hostname\_prefetch.csv
* hostname\_registry\_services.csv
* hostname\_named\_pipes.csv
* hostname\_processes.csv
* hostname\_processes\_dll.csv
* hostname\_startup.csv

According to the white paper by CERT SekoiaLab, it was in the above files where they managed to find the malware such as uroboros, ComRAT, Barbar, Casper, Poweliks and HDRoot.

When Cyber criminals attack, it is to their advantage to mess up the SIA and FNA timestamps in a Master File Table of applications. However, they may not be aware that the prefetch file also contain an unaltered version. Therefore, the Prefetch file can be used to pinpoint the real time stamps of applications.

Besides their primary purpose, prefetch files are useful for forensic examiners because they can prove that an application was installed and started on a particular machine.

A suspicious file would have one or more of the following characteristics, an unknown origin, located in system folders or unusual or hidden locations in the system, has unusual or misspelt names and contains obfuscated code. Therefore, by looking for these files which may fit the above conditions, we can form a list of files which may be malware.

**Visualisations needed**

Performance monitor vs time. This includes tracking service name and memory usage for each service.

The CSV and log files will be used for signature analysis.

Using FastIR, there are windows log events that cannot be extracted due to the below reasons:

*The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer.*

This needs to be debugged before being able to extract crucial information for log analysis.

**Comparison of FastIR with other IR tools**

There are many open source tools to develop in-house Security Information and Event Management (SIEM) tools available apart from FastIR. However, deeper exploration of FastIR is required before such tools can be compared. Some tools such as Sleuth Kit, BRO IDS had been mentioned by several authors. But looking at the objective of our solution, which is to conduct live forensic analysis quickly, perhaps FIR by CERT Societe Generale would be comparable.

**Useful links:**

**Tools, SIEMs, Partial Stacks**

<https://github.com/meirwah/awesome-incident-response>

<https://www.infoworld.com/article/2606779/security/163151-11-open-source-security-tools-catching-fire-on-GitHub.html#slide8>

<https://hackertarget.com/10-open-source-security-tools/>

<https://www.networkworld.com/article/3173690/security/how-to-assess-security-automation-tools.html>

<http://searchsecurity.techtarget.com/feature/How-to-buy-the-best-incident-response-tools-for-your-enterprise>

https://www.elastic.co/elasticon/tour/2015/washington-dc/cyber-security-log-analytics-at-decision-lab

<https://criticalstack.com/>

<https://github.com/criticalstack>

BRO IDS for network traffic:

<https://www.youtube.com/watch?v=R4QeuO1EX5o>

<https://www.slideshare.net/prajalkulkarni/attack-monitoring-using-elasticsearch-logstash-and-kibana>

<https://marcobonzanini.com/2015/08/10/building-a-search-as-you-type-feature-with-elasticsearch-angularjs-and-flask/>

**For Signature Analysis**

<https://www.virustotal.com/#/home/search>  
<http://www.team-cymru.org/about-us.html>

<https://virustotal.github.io/yara/>

Unique Approach to Threat analysis mapping: <https://www.youtube.com/watch?v=Fkqs28R13Y8>

Windows Systems and Artifacts in Digital Forensics, Part I: Registry: http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/#gref

**Network Analysis**

<http://searchsecurity.techtarget.com/podcast/Five-key-security-analytics-reports-and-how-to-build-them>

<https://www.elastic.co/blog/using-machine-learning-and-elasticsearch-for-security-analytics-deep-dive>

<https://cambridge-intelligence.com/use-cases-graph-visualization-cyber-security/>

**Malware Analysis**

<https://blogs.cisco.com/security/malware_validation_techniques>

<https://digital-forensics.sans.org/community/whitepapers>

<https://blog.cylance.com/blog/bid/297047/Uncommon-Event-Log-Analysis-for-Incident-Response-and-Forensic-Investigations>