**CIRTKit**

**Positive**

* Ongoing data collection

**Negative**

* Not full functions of the live forensics and incident system
* May not be capable of remote live forensics or scalable for enterprise

**Kibana (adopted)**

**Positive**

* Platform of analytics and visualization
* Better understanding of data
* Customize dashboard
* Review critical information without delay

**OSSEC**

**Positive**

* Real-time alerting
* Active response feature
* Automates the incident response process of blocking attacks
* Saving analysts time from chasing down attacks
* Blocking attacks manually
* Integratable

**Negative**

* Less customizable

**GRR Rapid Response (adopted)**

**Positive**

* Remote operation available
* Helps analysts collect and process data from numerous machines effectively
* Scalable architecture
* Lower the cost of response
* Increase the quality of evidence obtained
* Live forensics and incident response

**WFT**

**Positive**

* More comprehensive and sophisticated
* Scripted
* Minimize user interaction
* Report generator
* Instant generation of HTML format report during the data acquisition process

**Negative**

* Less scalable
* Users cannot change the programming code or revise the order of execution
* Have to download and bring along all the set of forensics programs

**Cyber Triage**

**Positive**

* Easily interpretable
* Agentless, fully automated
* Save time
* Process and generate report in real time

**Negative**

* No deep dive compatibilities on its own
* Cannot perform local analysis effectively

**Digital Forensics Framework**

**Positive**

* Modularity
* Improve software rapidly
* Scriptability
* Automated
* Possibility to extend features
* Genericity
* Compatible with multiple operating systems