Triage in Digital Forensics

By

Ryan Moore

Presented At

The Digital Forensic Research Conference

DFRWS 2012 USA Washington, DC (Aug 6th - 8th)

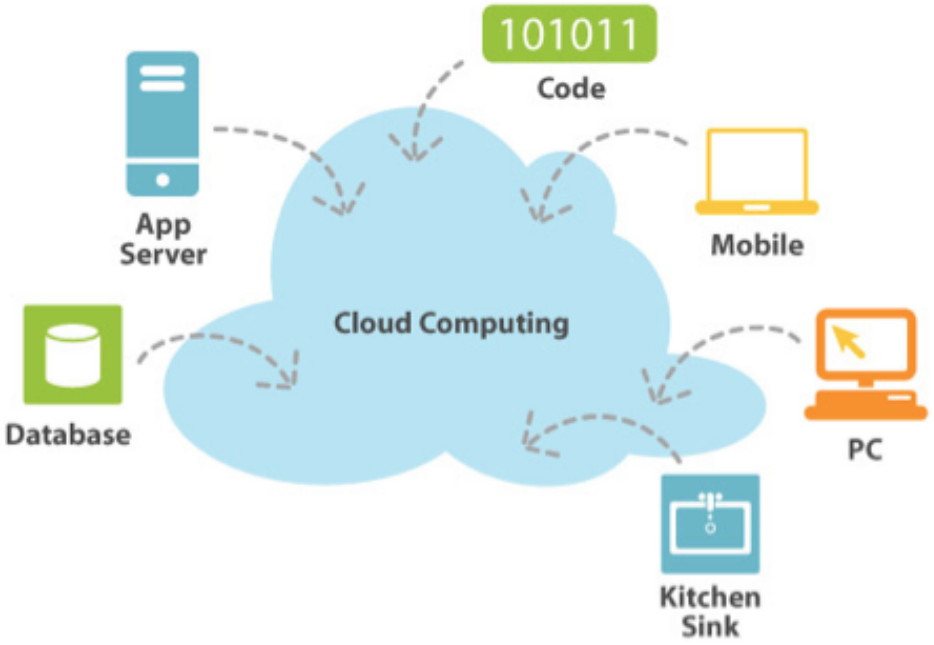
DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

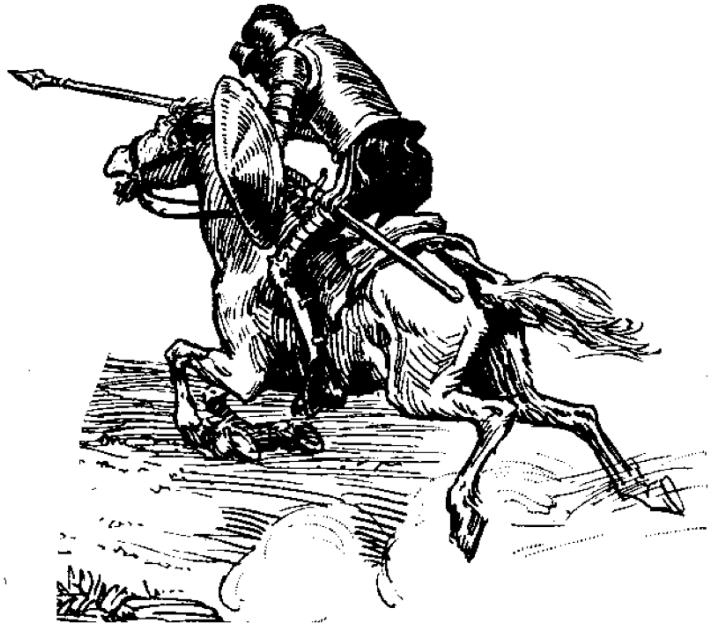
http:/dfrws.org

Digital Forensics Research Workshop

Triage in Digital Forensics

Why Triage?





Left hand picture: http://www.smallbiztechnology.com/archive/2011/09/wait-what-is-cloud-computing.html/
Right hand picture: http://forum.rollingstone.de/showthread.php?t=35030&page=29

Live Triage

- Mitigate risk to the acquisition process
- Identify next level artifacts
- Further suspect interview

Post Mortem Triage

- Interpret high pay-off artifacts without in depth forensic analysis
- Crowd source the analysis
- Identify next level artifacts

Remote Forensics

- Look at artifacts in a broader context
- Balance the work load
- Drop in expertise

Policy Considerations

- Competing legal standards
- Privacy considerations based on data type
- Exculpatory information

Triage in Digital Forensics

DISCUSSION