MOSAIKO …A TOOL FOR FORENSIC DATA ANALYSIS.

Tim Leschke, UMBC Cyber Defense Laboratory

Background:

Cyber forensics is the science of analyzing data from digital artifacts in such a way as to be able to testify about that data in a court of law.

Problem Statement:

The cyber forensic community is in a state of crisis because it does not have a tool that can keep pace with quickly changing technology.

State of the Art:

Current forensic tools are designed for use with specific digital artifacts. As such, these tools are not compatible with the newest technology. These tools also do not support meaningful forensic data analysis.

1. Current tools are not compatible with the most recent digital artifacts.

Solution:

- AT-commands
- Chip-off forensics
- Flexible communication

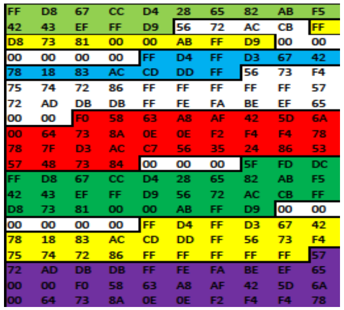
2. Current tools are not flexible enough to meet changing needs.

Bit Encoding	Hex
0011 0011 0000 0000	55 00
1001 1001 1000 0000	99 80

Solution:

- Do not hard-code rules
- Make no assumptions

3. Current tools do not draw attention to unknown data.

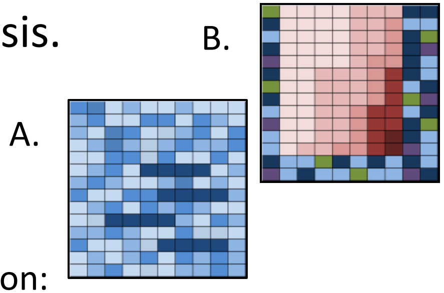


```
FF  D8  67  CC  D4  28  65  82  AB  F5
42  43  EF  FF  D9  56  72  AC  CB  FF
D8  73  81  00  00  AB  FF  D9  00  00
00  00  00  00  FF  D4  FF  D3  67  42
78  18  83  AC  CD  DD  FF  56  73  F4
75  74  72  86  FF  FF  FF  FF  FF  57
72  AD  DB  DB  FF  FE  FA  BE  EF  65
00  00  F0  58  63  A8  AF  42  5D  6A
00  64  73  8A  0E  0E  F2  F4  F4  78
78  7F  D3  AC  C7  56  35  24  86  53
57  48  73  84  00  00  00  5F  FD  DC
FF  D8  67  CC  D4  28  65  82  AB  F5
42  43  EF  FF  D9  56  72  AC  CB  FF
D8  73  81  00  00  AB  FF  D9  00  00
00  00  00  00  FF  D4  FF  D3  67  42
78  18  83  AC  CD  DD  FF  56  73  F4
75  74  72  86  FF  FF  FF  FF  FF  57
72  AD  DB  DB  FF  FE  FA  BE  EF  65
00  00  F0  58  63  A8  AF  42  5D  6A
00  64  73  8A  0E  0E  F2  F4  F4  78
```

Solution:

- Highlight known data

4. Current tools do not use visualization to support analysis.



Solution:

- Allow for the coloring of data based on content and meta-data

Conclusion:

The MOSAIKO research project will investigate the development of a tool that will be designed to interact with digital artifacts in a generic way. By being generic, the MOSAIKO tool will have the flexibility to be used with digital artifacts that employ the most recent digital technology.

The MOSAIKO tool will also provide data visualization in support of data analysis, which will speed-up the analysis process.

Future Work:

After the MOSAIKO tool is developed, future work will include the development of libraries in support of specific digital artifacts.

The *MOSAIKO* research project will develop a flexible tool to keep pace with quickly changing technology and support quicker analysis to meet the needs of the modern cyber forensic examiner.