TIERED FORENSICS METHODOLOGY MODEL FOR DIGITAL FIELD TRIAGE BY NON-DIGITAL EVIDENCE SPECIALISTS

BEN HITCHCOCK (ROYAL CANADIAN MOUNTED POLICE; UNIVERSITY COLLEGE DUBLIN)
NHEIN-AN LE-KHAC (SCHOOL OF COMPUTER SCIENCE, UNIVERSITY COLLEGE DUBLIN)
MARK SCANLON (SCHOOL OF COMPUTER SCIENCE, UNIVERSITY COLLEGE DUBLIN)

OVERVIEW

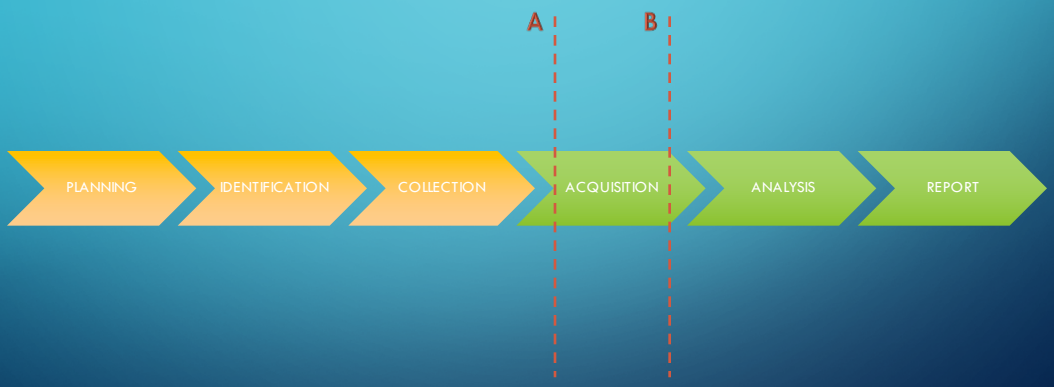
- Why the need of this approach?
- Digital Field Triage Model
- How the Model was implemented.
- Review
- Future work

WHY THE NEED TO CHANGE …

TIME DELAYS

- Society becoming more connected.
- "Do more with less".
- Backlogs created.
- Negative impact on operations
  - Right to a speed trial
  - Actionable intelligence when required
  - "Investigation delayed is Justice denied"

NATURAL BOTTLENECKS



OBJECTIVES

- Increase the efficiency of an investigation by providing artefacts from digital evidence in a timely manner.
- Decrease the backlog of files for analysis by Digital Evidence Specialists at a forensic laboratory.

DIGITAL FIELD TRIAGE

- Computer Forensics Field Triage Process Model (CFFTPM)
- Placing the Digital Evidence Specialist at the scene.
- Could some forensic analysis functions be downloaded?
- Discussion of a framework whereby this can be achieved.

THREE FUNDAMENTAL CONCEPTS

- DFT cannot work in isolation and must work with a parent TCU;
- DFT must maintain the forensic integrity of the digital evidence; and
- A DFT assessment does not replace a TCU analysis.

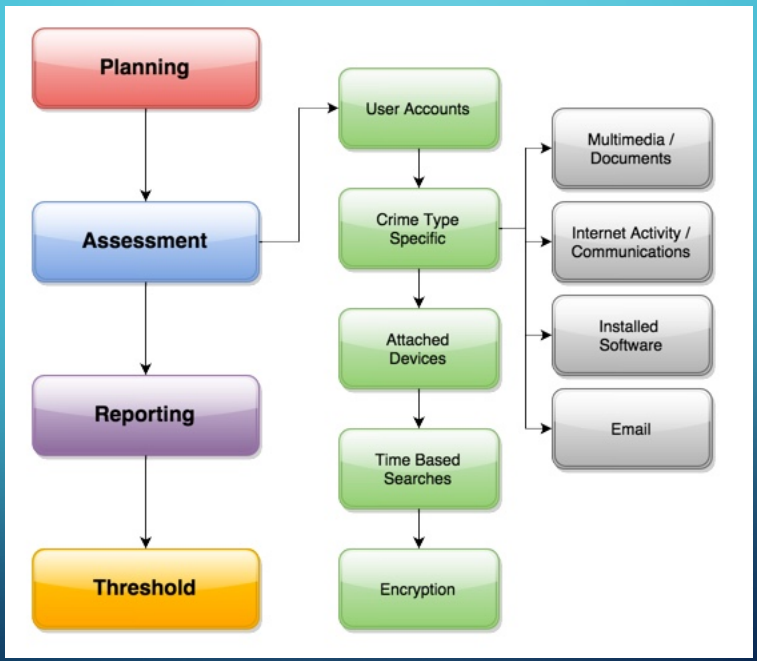
OVERVIEW OF ROLES

Assessment of Media — ***DFT Member***

- Does the digital evidence contain artifacts of the crime being investigated

Analysis — ***TCU Member***

- If the artifacts exist, where do they come from? How did the artifacts get there?
- Does the user of the digital evidence have knowledge of the artifacts?



BENEFITS – DFT MODEL

- Actionable intelligence when needed;
- Identifies relevant digital evidence;
- Ability for Prosecutor review earlier.

RISKS – DFT MODEL

- Excluding relevant evidence
- Absence of evidence / Encryption
- Risk not using the model – "*Sufficiency of Examination*"

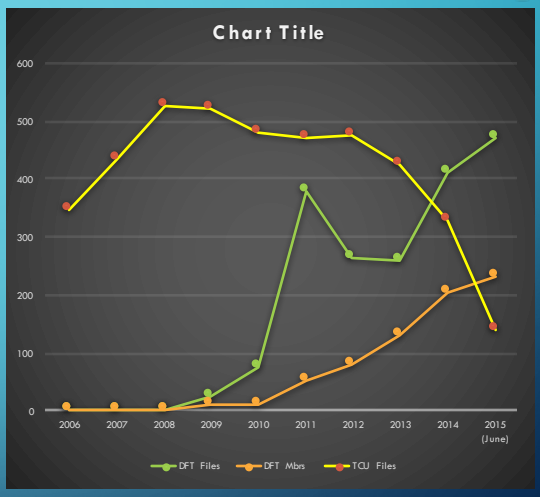
IMPLEMENTATION

- First applied 2009.
- Parent TCU
  - 25 Members (20 Digital Evidence Specialists)
  - Supported:
    - Population: 4.7 Million
    - Area: 945,000 km^2
    - 8,500 Employees (Federal, Provincial, Municipal)
    - 127 Police Stations (Size: 2 to 800 members)

DIGITAL FIELD TRIAGE

- Two business lines:
  - Digital Computer Field Triage
  - Digital Mobile Field Triage
- Dedicated Parent TCU Manager.
- Known pool for TCU recruitment

Year	DFT Files	DCFT Mbrs	DMFT Mbrs	TCU Files
2006	0	0	0	345
2007	0	0	0	435
2008	0	0	0	526
2009	26	9	0	522
2010	73	9	0	480
2011	376	53	0	468
2012	265	81	0	476
2013	260	104	24	422
2014	409	118	84	329
2015 (June)	469	118	96	137



REVIEW

- Improved efficiency
- Search scene to Local Station
- DCFT Custom Tool
- DFT Program constantly expanding
- Meets original requirements
  - Decrease in devices sent to TCU
  - Actionable intelligence in timely manner

OBJECTIVES

- Increase the efficiency of an investigation by providing artefacts from digital evidence in a timely manner.
- Decrease the backlog of files for analysis by Digital Evidence Specialists at a forensic laboratory.

FUTURE WORK

- Additional skills for DFT Members
- Better metrics
- Virtual training platform

"IT'S ALL ABOUT SURVIVAL NOW"

Rick Grimes – Walking Dead