Case Study

AccessData

Royal Military Police seeks out AccessData for Digital Forensics

Background

The Royal Military Police (RMP) Service Police Crime Bureau (SPCB) is the Army's technical investigative organisation. It has fifteen high-tech crime personnel within their Cyber Crime Centre (3C). Major Keith Miller, Officer Commanding SPCB, explains that because of the advanced digital forensics technology the RMP has built up, it is often called upon to assist with digital investigations undertaken by both civilian police and armed forces.

To put this into context, Major Miller explains that RMP handles between 100 to 150 cases a year with up to 15 devices seized for every individual investigated. The digital footprint of each case is 2 to 3 Terabytes of data with a single arrest involving the seizure and investigation of smartphones, laptops, USB drives, TVs, tablets and gaming devices, with gigabytes of data stored on each.

Previously, RMP officers used a dedicated tower computer for each case. Individual workstations could be tied up for days or weeks at a time working on a single case. This made collaboration difficult, which slowed down the analysis and presentation of digital forensic evidence. "This method is very inefficient because a single person works on that case and can't share the workload. If a machine crashes, or there is a power cut, the investigating officer may have to start the whole process again. This is still the situation for most forces."

Major Miller explains the human resource impact of this approach

"One officer had to single-handedly sift through 850,000 indecent images to compile evidence for a case. Why put an individual through that mental strain when there are smarter, digital ways of completing this task?"

Major Keith Miller, Officer Commanding SPCB commenting on the unnecessary burden put on human resources before discovering Digital Forensics from AccessData

Solution

RMP SPCB has developed a global centre of cyber-crime expertise, which uses a collection of high powered servers and leading digital forensics software to ingest, process, analyze and archive data from suspects' devices. 'ARES' is a combination of leading edge hardware and software used by all of the forces to process digital evidence for early case assessment and prosecution.

Major Miller reports that ARES has refined the digital forensic investigation process within 3C, and in particular has revolutionised collaborative working. (See diagram on back)

Result

AccessData Lab, powered by AccessData'sForensic Toolkit® (FTK®) is the technology, used by all 3C staff to process and analyze potential evidence. AD Lab also allows multiple investigators to work collaboratively in real time, via a Web interface to achieve more efficient early case assessment.

"Previously, the digital forensics toolset we were using did not allow personnel to share a centralized investigative infrastructure," states Major Miller, "While we have always used FTK as part of our toolset, AccessData Lab was only introduced to the ARES system eighteen months ago. It provides us with distributed processing, which is a new way of working that allows us to handle very large volumes of data very quickly."

"FTK and AD Lab enable us to use ARES to its full capability, allowing us to quickly train investigators to use the interface and collaborate on early case assessment. This frees up highly qualified digital forensics analysts to focus on analysis."

Major Miller cites the benefit of using FTK and AD Lab to automate the collaborative process of early case assessment. "When you get into early case assessment, why use a highly trained analyst to do this, when the investigator should be doing the job, as it is they who are intimate with the nuances of the case?"

Summary

The 3C reduced its caseload of historical jobs by 42 percent in the first 4 months of use because it was able to ingest all jobs at point of receipt and allocate collaboratively. Moreover, 3C has been able to apply its expensive analyst resources at the right point of the investigation, thereby increasing productivity. 3C has also been able to explore numerous additional lines of enquiry that have only been made possible by involving investigators in early case assessment.

ARES has driven the fiscal cost of an indicative case from GBP £9,500 down to GBP £3,200.

THE BOTTOM LINE

ARES Process Overview

MP

ARMY

★ = IMR

SPCB 3C Ownership

Exhibits submitted to the 3C with a submission form detailing what evidence is sought and current lines of enquiry and immediate concerns. A case evaluation is conducted by the WOIC, ECA Coordinator and Team Leader and an Ingestion Plan is produced for each case by the WOIC.

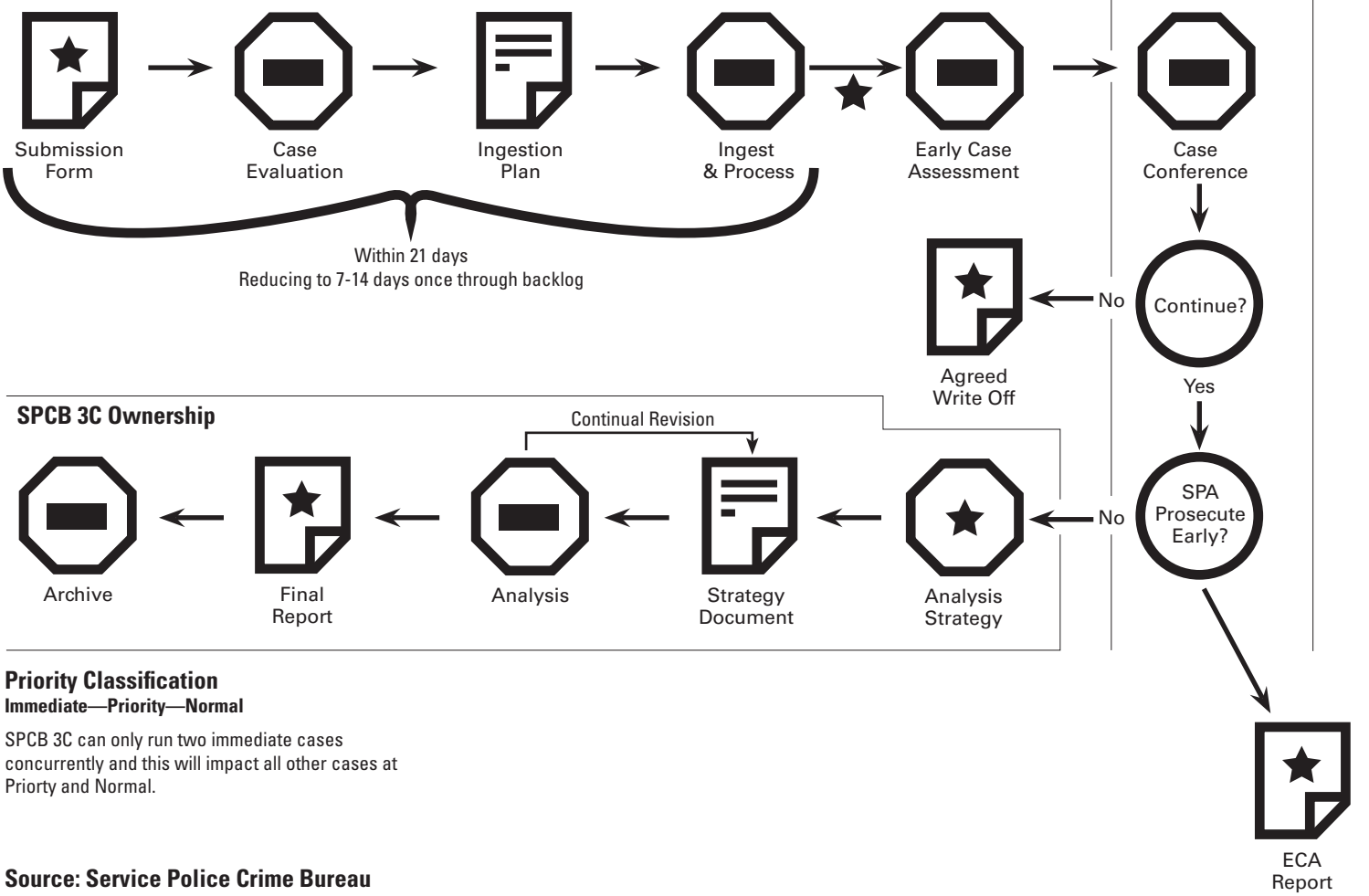
Imaging and processing of all exhibits in FTK (except Mobile Phones that cannot be imaged), with guidance from the Ingestion Plan, implemented by the Team Leader and then back to the ECA Coordinator.

Investigator Ownership

Investigators review the case with assistance from the ECA coordinator and identify data that they require as evidence.

Joint Ownership

ECA report can be produced, SPA can decide to prosecute at this point, if evidence is overwhelming or conversely SIB can write off investigation.



Priority Classification

Immediate—Priority—Normal

SPCB 3C can only run two immediate cases concurrently and this will impact all other cases at Priorty and Normal.

Source: Service Police Crime Bureau

AccessData

CORPORATE HEADQUARTERS
801.377.5410
588 West 400 South
Suite 350
Lindon, UT 84042 USA

NORTH AMERICAN SALES
800.574.5199
801.765.4370
sales@accessdata.com

INTERNATIONAL SALES
+44 (0)20 7010 7800
internationalsales@accessdata.com

www.accessdata.com