Van: https://www.helpnetsecurity.com/2013/12/23/breaking-the-backlog-of-digital-forensic-evidence/

Dr. Hans Henseler, Founder of the Forensic Computer Investigation Department at the Netherlands Forensic InstituteDecember 23, 2013

Breaking the backlog of digital forensic evidence

It is time for a change in the way the law enforcement works with digital forensic evidence. Every police investigator needs to be able to quickly and easily analyze digital forensic evidence related to their criminal cases—• from photos, videos, email, social media and Internet usage to audio and documents.

And each day that a computer or mobile device sits in a police department's backlog waiting to be processed is one that a criminal remains on the street.

Electronic devices routinely contain evidence related in some way to the planning, coordination, commission or witnessing of crimes. And the digital information contained in seized devices is typically sent to specialists in digital forensics laboratories to be processed.

Explosion of digital forensic evidence

Today digital forensics laboratories alone can no longer manage the sheer volume of digital evidence in criminal cases. The backlog of caseloads from law enforcement agencies has grown from weeks to months worldwide. Digital forensic specialists cannot be trained fast enough and the number of specialists required to analyze the mountains of digital evidence in common crimes is simply beyond budget constraints.

According to Luc Beirens, Superintendent of the Federal Computer Crime Unit (FCCU) in Belgium, "the number of seized computers is a multitude of the number that was seized ten years ago. Every person that we search probably owns a desktop computer, a laptop, an iPad, and a smart phone and in addition you may see a pile of external hard disks. All those systems need to be investigated."

But of equal or perhaps more importance is that sending digital evidence to specialists takes the critical parts of criminal investigations out of the hands of investigators.

Typically, the digital information related to a case requires the detective's knowledge to determine what information may be relevant and what clearly is not. New tools to triage digital evidence in the field exist, but the capabilities are limited and investigators must still deal with the difficulties of explaining evidence to the digital forensic specialists.

These specialists can examine evidence—• when they can get to it—• but not in the context of the case or how digital traces relate to other evidence. Not even investigators can know exactly how digital evidence will emerge or its value to a case until they see it themselves.

A targeted, local approach to digital investigations

The Police Zone Schelde-Leie in the East Flanders province of Belgium recently caught a thief red-handed in a store. He defended himself with the classic excuse—• he had never stolen anything and he would never do it again. No stolen goods were found during a search of his home and normally the police would have to swallow his excuse. But this time was different.

Since June the Schelde-Leie police unit has been using new software technology that allows non-technical investigators to process and analyze digital forensic evidence.

The detectives seized the thief's computer and found on the hard drive photos of other stolen goods that the man had posted on a classified advertisement site.

Police Zone Schelde-Leie is a small police unit but very sophisticated. Because they were fed up with waiting three to six months for results from the federal computer crime units they became the first local Belgian Police Zone to use software to extract data from mobile phones.

The De Pinte police unit is among a growing base of law enforcement units worldwide using new web-based software solutions, to enable their non-technical detectives to quickly process and extract valuable information from seized mobile devices and computers—• without having to wait for the digital experts in the forensic lab.

Since they began using their new software solution in May of this year they have seized more devices and have processed well over 10 terabytes of data. In fact, in the first two weeks alone investigators were able to process four cases with twelve containers of evidence. Normally this would take the police unit months to accomplish.

Luc Luyckx, a detective from the police unit at Schelde-Leie was concerned about accessing and potentially altering digital evidence. For example when viewing photo files the "last date viewed' element could change. They can now bypass the login codes and make a forensic copy so investigators can process and analyze the data but they cannot change the original files or compromise their evidence.

In addition, a forensic copy or image of the suspect computer can be sent to digital forensic experts for a deep dive investigation so that the computer (or other electronic devices) can be returned to the owners in the absence of obvious evidence.

Their new anti-crime software program also helped detectives in De Pinte quickly solve another criminal case and this time in defense of a suspect.

The parents of an under-aged girl were very worried. Their daughter was asked in computer chats to perform sexual acts. Analysis of the digital data showed that the conversations were indeed sexually charged, however the daughter was also to blame for her participation. Luyckx added, "We started that case in August, and the investigation is already finished. Normally we would still be waiting for the computer."

According to Hans Henseler, the founder of the Computer Forensics section of the Netherlands Forensic Institute and a Program Manager at Fox-IT, a digital investigation firm, detectives who best know the case can now sort through evidence themselves leaving mobile and computer forensic experts to work on what they know and do best.

This enables a more targeted approach to the investigation of digital evidence and a more efficient use of forensic laboratories.

Dr. Hans Henseler, founder of the Forensic Computer Investigation Department at the Netherlands Forensic Institute, managing partner of the Forensics Business Unit at Fox-IT, and a professor of e-discovery at the Hogeschool in Amsterdam.