RSA CONFERENCE ASIA PACIFIC 2013

Security in knowledge

AN INVESTIGATION INTO THE METHODS USED FOR TRAFFICKING OF CHILD ABUSE MATERIAL

Dr. Allan Charles Watt, PhD, CFCE, CFE
Macquarie University, Sydney, Australia

Session ID: CLE-W02

Session Classification: Intermediate

What sought of Kangaroo is that?

Background

- NZ Army (Royal New Zealand Infantry Regiment) 9 years
- NZ Police (Sworn Police Officer/ Intelligence Analyst) 9 years
- Computer Forensic Investigations (NZ) 10 years
- E.law International, Sydney (Head of e.forensics) 3 years
- NSW Police (Electronic Evidence Specialist) 2 years
- Macquarie University (Adjunct Lecturer) 18 months
- Macquarie University (Cyber Program Coordinator/Lecturer) 1 Month (still have training wheels on)
- Completed over 1000 computer forensic investigations since 1995.

Academic

- Diploma in Policing
- Bachelor of Business Studies (Accounting)
- Bachelor of Science (Information Systems)
- Post Graduate Diploma in Forensic Science
- Master of Science in Forensic Science (Thesis Cyber Terrorism)
- Doctor of Philosophy (Child Abuse Material)
- Certified Forensic Computer Examiner
- Certified Fraud Examiner

Research

- This presentation is based on research into, the trafficking and concealment of Child Abuse Material (CAM).
- Used to be called Child Pornography.
- Why CAM?
- Research shows and also from my experience through a number of investigations in LE, it is known that those who traffic or possess CAM, do not do it just once.
- They also have many files (1000s) and catalogue them.
- Therefore rather than develop a model for investigating anything on a computer, this research focused on something specific as in image files, still or moving.

Child Abuse Material

- Lastly CAM is not about still or movie files, it is about the sexual abuse of children and every bit of research towards stemming the flow helps.
- The following are all intertwined
  - Human Trafficking of Children
  - Child Sex Slaves
  - Child Sex Tourism
  - Child Abuse Material Creation
  - Child Abuse Material Distribution/Trafficking/Possession
- If we slow the demand, then we will reduce the supply
- How? Increase the investigators skills

What the Research Covered

- An assessment from research and questionnaires on what agencies specialise in CAM, globally and regionally
- Collected primary and secondary statistics on CAM, possession and trafficking
- Collected primary case studies from Law Enforcement from around the world on CAM cases.
- Based on those cases, technical testing of various methods of file movement and concealment were conducted.
- There were other areas that could have been tested, however as they did not feature as mainstream methods they were not covered.

Methodology

- 135 separate tests were conducted in both Windows 7 and Windows XP, on different ways to conceal or move files.
- After each test, the system drive was forensically imaged and the same system drive then received a fresh install restored over the top, prior to the next test being conducted.
- This way there were no extraneous variables to interfere with the results.
- On completion of the testing each of the 135 forensic images were analysed with forensic tools, Encase, FTK, IEF.
- Observations were noted and the results were recorded.

Research outcome sought

- Provide three frameworks to assist investigators in CAM trafficking and concealment cases:
  - Crime scene actions
  - Analysis for possession evidence
  - Analysis for trafficking evidence
- Provides a reference model for investigators and that in some cases eliminates the need to conduct testing.
- Reducing valuable time.
- Allows less experience staff to conduct triage on devices that potentially may contain CAM evidence.

Trafficking

- As the research was large, it is not possible to present all of it in one session, so this specific session is focusing on the trafficking framework and presents the highlighted points for a number of protocols.
- There were two aspects:
  - Observations from the testing
  - Analysis of the observations
- The following is a framework for investigating file movement, some of which is non volatile, in that the files moved will be present still at one end of the movement activity or those that are volatile, such as when a live video is streamed over the Internet and only residual data may be present.

General File Movement

- As is the norm with both of the Windows operating systems tested, most files that are saved directly to the local HDD or other storage media attached to the device will have the relevant files names recorded in the File System Management Files (FSMF), these being, '$LogFile', '$MFT' and '$UsnJrl.$J'.
- Or in FAT systems, the FAT tables or Folder remnants in unallocated clusters.
- Hence FSMF was the acronym used to cover the principle file name storage files.

FTP Download

- Should it be suspected that the files were obtained by FTP, then some evidence will exist. That is, use of 'FTP.exe' in the Windows Registry and Event logs, primarily the firewall and security related events. It is possible the IP Address of the computer that was connected to will be contained within the 'BootCKCL.etl' file within Windows 7.

HTTP Download

- For a HTTP download, the various browser history files will need to be assessed as these will provide the name of the site visited and the files downloaded. In Windows 7, with the Internet Explorer download, there will be likely references in the 'Jumplist' file.

- If the download occurred with the browser in Private Browsing mode, though there will be references to the files downloaded, it is unlikely any reference to the website visited will appear anywhere on the devices.

Live Streaming Video Download

- In Windows 7 with the Internet Explorer download, there will likely be references in the 'Jumplist' file. The pagefile, may also provide some reference to the name of the video viewed, if it is known. If the video was viewed live via UDP there will be no copies of the frames present on the device.
- If the download occurred with the browser in Private Browsing mode, there will no references to the video, it is also unlikely any reference to the website visited will appear anywhere on the device. However references to the name of the video may be located in the pagefile if it is a Windows XP device.

Viewing a Picture on a Website

- The most evidence that will be located will be one where the browser used is Internet Explorer, not only will the picture that was viewed be downloaded to the temporary Internet files, but so were all the other thumbnails on the pages that was visited.
- With the private Browsing there will be no reference to the website, the picture viewed or copies of the picture anywhere.

Viewing a Picture on a Website using an Anonymiser

- When an anonymiser was used, it is likely no evidence will be located with the ISP, due to a proxy being used.
- However, evidence of the website visited and the name of the picture will be present in the browser history files.
- If Private Browsing was used there will be no evidence in the history files under Windows 7, however there may be some under Windows XP of the proxy access only and not the website visited beyond that.

Peer-2-Peer (P2P) File Sharing

- Most of the P2P applications will have an associated database and these will be located usually under the relevant user's profile logged into at the time the specific files were downloaded.
- An assessment of the applications installed will show if a P2P application has been installed.
- The tests were conducted on the 'Shareaza' P2P application and this application recorded activity in the following files:
  - CurrentDatabase_372.wmdb
  - DownloadFile.db
  - ContentFile.db

P2P

- The 'Shared' folder that is common to P2P applications is also another place that needs to be assessed for files that have been downloaded or files that have been placed there for sharing with other users.
- In some cases, it may be necessary to assess the activity of the P2P running live so a defence of the 'Shared Folder' was not set to ‘display’ can be raised.

Webmail Transfer

- With Gmail transfers, regardless whether they were sent from another Webmail, a POP application or an iPhone, little detail will be found about the content of the email other than access to the Gmail site itself was made.
- Access to the files that were sent by webmail is also not likely to be present in Windows 7, but will be in Windows XP.
- Reference to the email addresses in the communication should be located in the history files for both sending and receiving and on a receiving device, reference to the files that were part of the email should also be located in the history files.

Cloud Storage

- With many cloud applications like Dropbox and GigaTribe, the presence of the application as having been installed is often an indicator that some cloud storage may be in existence. Windows registry activity will also show if they are automatically open on start up and also the last time they were used.
- Similar to a 'Shared Folder' with the P2P applications, these types of Cloud applications create a similar folder and when the user copies files to their Cloud, it will copy them to this folder first and then upload them from there.
- If access to the Cloud is directly through private browsing and the files are also being viewed from the Cloud and not actively downloaded to the end user's device, it is unlikely any reference to the site will exist nor the picture or videos that were viewed on the cloud site.
- If the cloud being accessed is not a main stream cloud application and is essentially a network site, then access to this may be recorded in the Internet history files. If the connection is by RDP then there will be reference to this in the relevant '.rdp' file.

Skype Communications

- Provided the recording of user activity has not been turned off, the Skype data files, primarily 'main.db', under the user's profile folders, will record the details of the users, contacts, copies of any calls that were made.
- Any text based communications, including the actual text and if any files were transferred.
- Copies of the communications may also be found within the pagefile.

Facebook Communications

- For Facebook investigations where Google Chrome or a private browser and Windows 7 is used there is unlikely to be any remnants of the communications or any other activity, other than a screen shot of the first page visited within Facebook in the history files.
- Within Windows XP, there will be references to the names of the two parties involved in the communications as well as text of the conversation. A forensic tool like Internet Evidence Finder (IEF), will be able to attempt a recovery of the communications

MSN

- Details of contacts for the user's account should be found within the 'ContactsLog.txt' file. An 'XML' file will also be created that will have recorded the text of the communications, the parties involved in it and the details of any files that were transferred. It is also possible copies of any communications will also exist in the pagefile. As MSN and Hotmail are Microsoft products, relevant data is also present in Internet Explorer's 'Index.dat' file.
- It is likely the IP Address of the remote computer involved in the various computers will also be present.

Freenet File Transfer

- Freenet, like some of the Cloud applications, requires a local install of the application. The presence of the application should be an indication of further evidence and the Windows Registry should hold evidence as to any recent use.
- The user name for account holder for the installation is recorded in the 'freenet.ini' file. Some detail about the other parties user details and their IP address is likely to have been captured in a Freenet local support file, 'openpeers-#####'.
- As was shown in the tests, when Freenet starts, it does so using a Google Incognito, private browser Window and as shown with the use of this browser, there is no remnant data from its use.

Internal File Transfer

- Within the 'SYSTEM' and 'USER' hives of the Windows Registry will be recorded the IP address of the remote computer that pushes the files, but not on the computer receiving the files.
- The Event logs will also show activity of a network transfer, but only within Windows 7.
- Other than the presence of link files for the files transferred, no other data will be present.

BitTorrent Download

- The presence of the BitTorrent application will be an indicator that more evidence of BitTorrent downloads may exist.

- Beyond this evidence of files downloaded and other partial details will be located in the following files:
  - SystemIndex.3.gtr
  - dht.dat
  - resume.dat
  - rss.dat
  - settings.dat

ICloud Activity

- The presence of the Apple iCloud application will be an indicator that it may have been used to transfer files. Further detail can be obtained from reviewing the 'local.db' files under the user's profile folders. This file will contain the details of any files that have been transferred.
- No other valuable evidence is likely to be located on the computer other than the iPhone's name.

Trojan and Metasploit Attack Investigations

- Details of the attack may be recorded in the antivirus logs or the event logs primarily for Windows 7.
- If the relevant time of the attack is known or the name of the applet that was the agent that allowed the Trojan attack, then this may assist in locating the files.
- If this detail is not located and no other connectivity data from the ISP or Routers, then it is possible no data will be available to confirm or deny that a Trojan attack did occur.

Trojan and Metasploit Attack Investigations

- It may be then necessary to scan the Windows registry to identify files that are activated on start up and then locate each one of these individually and determine if they are in fact Malware.
- Should the applet be located it may be possible to locate the IP address of the attacking computer, the 'Client', from within it.

Trojan and Metasploit Attack Investigations

- The difficulty with a computer that has been the victim of a Trojan type attack, is once the connectivity has been made, it is difficult to decipher what was completed locally and what was completed as a result of remote instructions sent to the computer.
- If the presence of a Trojan is found during an investigation, a test environment needs to be established and the Trojan, Client/Server environment created and tests conducted.
- As was found in the tests, it is possible to deploy the agent applet and then copy files across without causing a live notification to the device. Given this, the Trojan Horse defence for some specific Trojans is feasible.

Bluetooth

- There will be references to presence of the Bluetooth application. This however will be standard if the device comes fitted with Bluetooth hardware. The Windows registry will also identify if the Bluetooth application is on or off by default. However if it is being turned on and off manually it may not be possible to determine if it was actually on or off at a specific time.
- It should also be possible to locate the name of the other device that was connected, as past devices are retained under the user's profile and the Windows registry. A Bluetooth folder will also be located under the 'My Documents' folder within the user's profile, this being the default location for files if they are pulled or pushed to the device.

Virtual Network Connect

- Though the presence of the remote software existed and that connectivity occurred, there is little evidence present to show what was done locally and what was done remotely, thereby leaving little evidence to decipher between the two. The presence of the application would be similar to investigating an attack by way of a Trojan Horse and identifying what was done locally and what was done remotely is a difficult process to conduct.

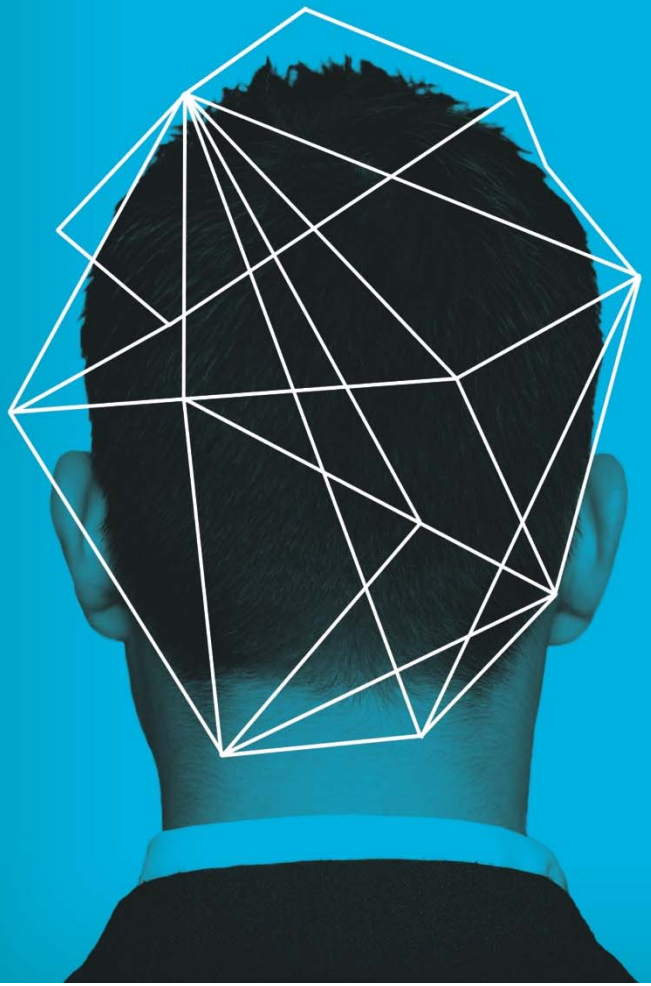
Conclusions

- We are all creatures of habit and computer users take steps to secure there browsing or storage activity, so they can repeatedly look at the files they have downloaded. As a result there will be an abundance of evidence present.
- If however private browsing is used, an anonymiser or a remote private cloud, there may be little or no evidence present.
- It is also possible to attack another computer with a Trojan Horse, plant a file and get out without being detected, which could add weight to those attempting to raise the Trojan Horse Defence in Child Abuse Material Possession cases.

Summary

- Whether there is a law in a state nation or not, Child Sex Abuse is a crime.
- Therefore the distribution of material portraying children being sexually abused is also criminal.
- The digital age has allowed this offending to be proliferated.
- Digital devices contain digital DNA, that we need to use to extract intelligence and seek the source of this material.
- This will be a start towards locating the source of the material and stemming the supply.

RSA CONFERENCE ASIA PACIFIC 2013



Aussie, Aussie, Aussie...Oi, Oi, Oi