TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE

សន្និសីទបណ្តុះបណ្តាលអំពីការធ្វើអាជីវកម្មផ្លូវភេទលើកុមារកម្ពុជា (ខែកក្កដា ២០១៩)
ការធ្វើកោសលវិច័យឌីជីថុល

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE

ទស្សនវិស័យនៃកិច្ចប្រជុំ

- កិច្ចប្រជុំនេះនឹងគ្របដណ្តប់លើតួនាទីនៃការធ្វើកោសលវិច័យការស៊ើបអង្កេតការធ្វើអាជីវកម្មផ្លូវភេទលើកុមារ មានដូចខាងក្រោម៖
  - តើការធ្វើកោសលវិច័យឌីជីថុលជាអ្វី (Digital Forensic = DF)?
  - តើសមត្ថភាពកោសលវិច័យឌីជីថុលរបស់នគរបាលសហព័ន្ធអូស្ត្រាលី (AFP) និងនគរបាលជាតិកម្ពុជា (CNP) មានអ្វីខ្លះ?
  - និន្នាការ និងបញ្ហានាពេលបច្ចុប្បន្ន
  - ឧទាហរណ៍ឆែកឆេរ - សារៈសំខាន់នៃការធ្វើកោសលវិច័យឌីជីថុល
  - ស្តង់ដាអន្តរជាតិ និង ការទទួលយកភស្តុតាង
  - សេចក្តីថ្លែងការ និងរបាយការណ៍ AFP DF សម្រាប់តុលាការ
- បន្ថែម, ការបង្ហាញឡើងវិញ (ការទទួលបាន ការវិភាគ ។ល។) ដើម្បីការយល់ដឹងរបស់អ្នកអំពីឧបករណ៍កោសលវិច័យឌីជីថុល និង
ការយល់ដឹងអំពីឧបករណ៍ និងបច្ចេកទេស

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

គោលបំណងសំខាន់នៃកិច្ចប្រជុំនេះ...

- ខ្ញុំចង់បង្ហាញអ្នកអំពី<u>ទស្សនវិស័យនិងការលើកកម្ពស់ការយល់ដឹងអំពី</u>:
  - សារៈខាន់នៃការធ្វើកោសលវិច័យ
    - ការចូលរួមនីមួយៗ
    - ការចូលរួមភ្លាមៗក្នុងការស៊ើបអង្កេត
    - ដីកាឆែកឆេរ(មុនការវីបអូស)
    - មន្ទីរពិសោធន៍ (ក្រោយការវីបអូស)
  - សមត្ថភាពបច្ចេកទេសកោសលវិច័យ
  - CNP DF – ការប្រើប្រាស់ (ទាំងនេះសម្រាប់អ្នកឯកទេស)
- កោសលវិច័យឌីជីថុលថ្មីសម្រាប់កម្ពុជា
- ប្រទេសកម្ពុជាកំពុងចាប់ផ្តើមការគិតគូររបស់ខ្លួនអំពីការប្រឆាំងបច្ចេកវិជ្ជា

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ឥឡូវចាប់ផ្តើម ជាមួយការងារសំខាន់ៗខាងស្តិតិ!

TRAINING-IN-CONFIDENCE

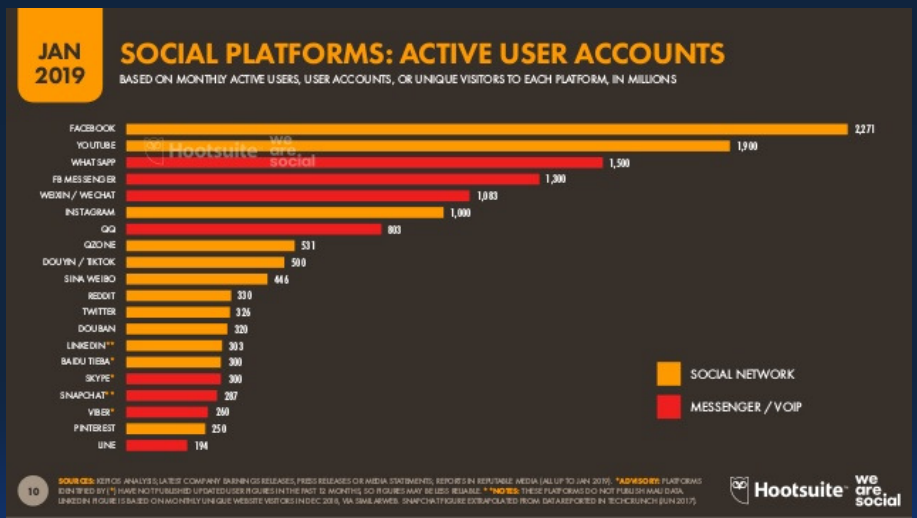
TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE



TRAINING-IN-CONFIDENCE

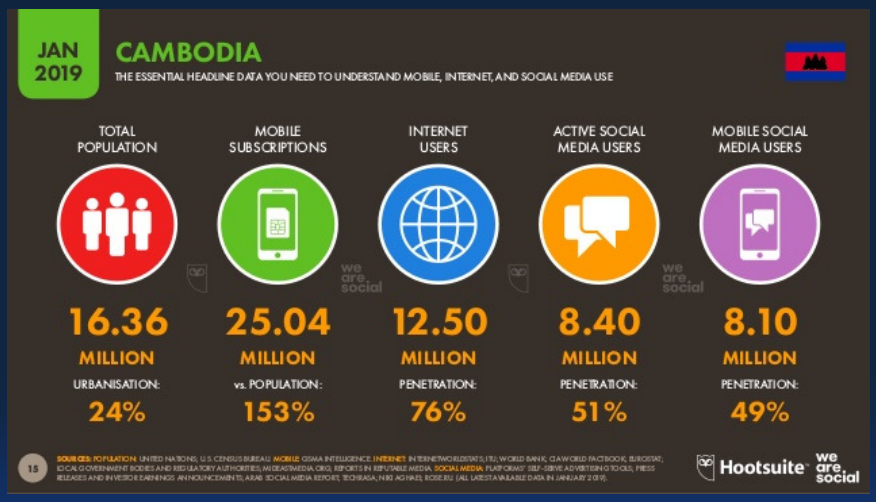
TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

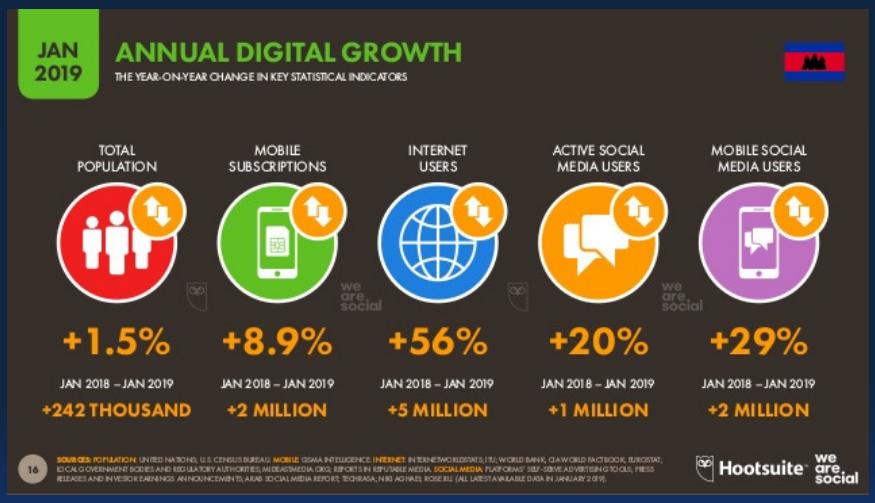
AFP
AUSTRALIAN FEDERAL POLICE



TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

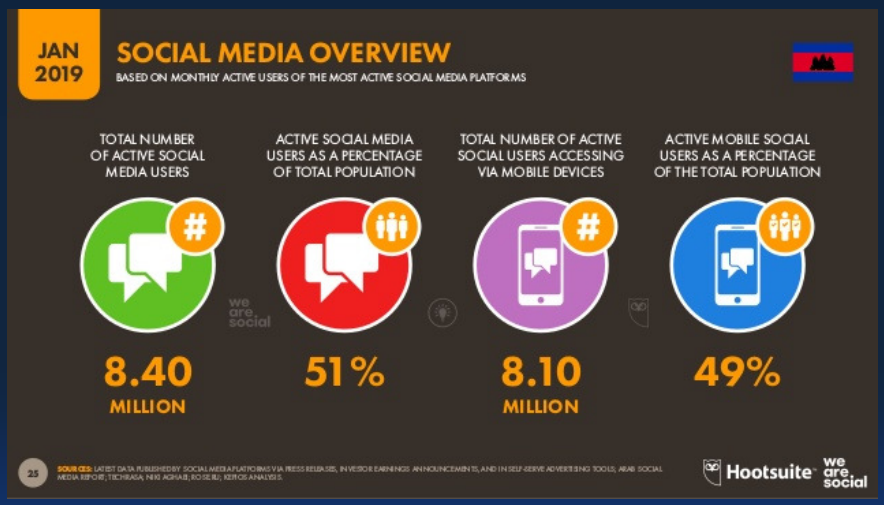
AFP
AUSTRALIAN FEDERAL POLICE



TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE



TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

តើកោសលវិច័យឌីជីថុលជាអ្វី?

កោសលវិច័យឌីជីថុលគឺជាការការពារ ការទទួលយក/ចាប់យក និងការវិភាគទិន្នន័យដោយប្រើប្រាស់គ្រឿងអេឡិចត្រូនិច្ច ដូចជា កុំព្យូទ័រ អង្គផ្ទុកព័ត៌មាន/ឯកសារ និងទូរស័ព្ទចល័ត

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

តួនាទីអ្នកធ្វើកោសលវិច័យតាមឌីជីថុល

- មានវត្តមាននៅពេលមានដីការឆែកឆេរ
- ពិនិត្យ៖ CCTV, កុំព្យូទ័រ ទូរស័ព្ទចល័ត ម៉ាស៊ីនព្រីន PDAs, USB និងគ្រឿងអេឡិចត្រូនិច្ចផ្សេងទៀតដែលអាចជាភស្តុតាង
- ទាញយកសម្លេងថតពីឧបករណ៍អេឡិចត្រូនិច្ចដែលជាភស្តុតាង/
- ទាញយកទិន្នន័យ (ឯកសារដែលបានលុប)
- ទាញរក ផាសវើត (Password recovery) និងអក្សរសម្ងាត់
- បកស្រាយឧបករណ៍ព័ត៌មានភស្តុតាង និងរបាយការណ៍ផលិតកម្ម
- ចូលរួមក្នុងនីតិវិធីតុលាការដើម្បីផ្តល់ទស្សន ជំនាញជាក់ស្តែង

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

វដ្តនៃការស៊ើបអង្កេតបែបអេឡិចត្រូនិច

- ការធ្វើផែនការ
- វត្តមាននៅកន្លែងកើតហេតុឧក្រិដ្ឋ
- ការកំនត់អត្តសញ្ញាណ
- ការពារ/យកមកក្សា
- ទទួលយកជាភស្តុតាង
- ដំណើរការ
- ធ្វើកោសលវិច័យ
- ធ្វើរបាយការណ៍
- ផ្តល់សក្ខីកម្មនៅតុលាការ

មុនពេលរឹបអូស

ក្រោយពេលរឹបអូស

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

វដ្តនៃការស៊ើបអង្កេតបែបអេឡិចត្រូនិច

- ការធ្វើផែនការ
- វត្តមាននៅកន្លែងកើតហេតុឧក្រិដ្ឋ
- ការធ្វើអត្តសញ្ញាណកម្ម
- ការពារ/យកមកក្សា
- ទទួលយកជាភស្តុតាង
- ដំណើរការ
- ធ្វើកោសលវិច័យ
- ធ្វើរបាយការណ៍
- ផ្តល់សក្ខីកម្មនៅតុលាការ

អនុវត្តឡើងវិញទិន្នន័យកោសលវិច័យអេឡិចត្រូនិច

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

កោសលវិច័យឌីជីថុល AFP - ទីកន្លែង

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

តើអ្នកណាគាំទ្រការងារកោសលវិច័យឌីជីថុល AFP?

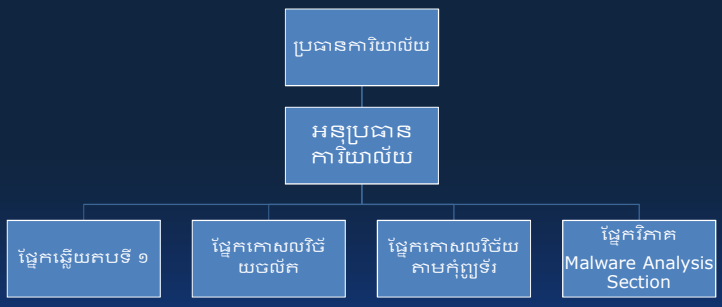
- ការគាំទ្រការងារកោសលវិច័យឌីជីថុលរបស់ AFP តាមប្រភេទនៃការស៊ើអង្កេតដូចខាងក្រោម៖
  - ការប្រឆាំងភេរវកម្ម
  - ការធ្វើអាជីវកម្មផ្លូវភេទលើកុមារ
  - ឧក្រិដ្ឋកម្មបច្ចេកវិជ្ជា
  - ការរត់ពន្ធមនុស្ស
  - ការគេងបន្លំ និងអំពើពុករលួយ
  - គ្រឿងញៀន (ការនាំចូល/នាំចេញ)
  - កិច្ចសហប្រតិបត្តិការអន្តរជាតិ

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការធ្វើកោសលវិច័យឌីជីថុលរបស់ CNP

- ជាផ្នែកមួយនៃនាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិជ្ជាដែលបានបង្កើតឡើងក្នុងខែកញ្ញា ឆ្នាំ២០១៥
- ខាងក្រោមនេះគឺជារចនាសម្ព័ន្ធក្រុមកោសលវិច័យឌីជីថុលរបស់នគរបាលកម្ពុជា



TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការទទួលយកភស្តុតាងកោសលវិច័យឌីជីថុលនៅក្នុងតុលាការ

ការទទួលយក - គុណភាពដែលអាចទទួលយកបាន ឬ យកជាការបាន

- ស្តង់ដាមូលដ្ឋានក្នុងការធ្វើកោសលវិច័យរួមមាន៖
  - ភាពមូលនៃទិន្នន័យ ឧទាហរណ៍៖ write-protection, hashing
  - ការជឿងផ្ទាត់លទ្ធផល
  - ខ្សែសង្វាក់នៃគោលការឃុំឃាំង
  - ការរកឃើញដដែលៗ/ដូចៗគ្នា
  - គុណភាពនៃរបាយការណ៍កោសលវិច័យ
- ***យើងនឹងសិក្សាចំណុចនេះឲ្យបានលម្អិតជាងនេះទៀតក្នុងវគ្គនេះ***

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ប្រភពភស្តុតាងពីគ្រឿងអេឡិចត្រូនិច

TRAINING-IN-CONFIDENCE

AFP

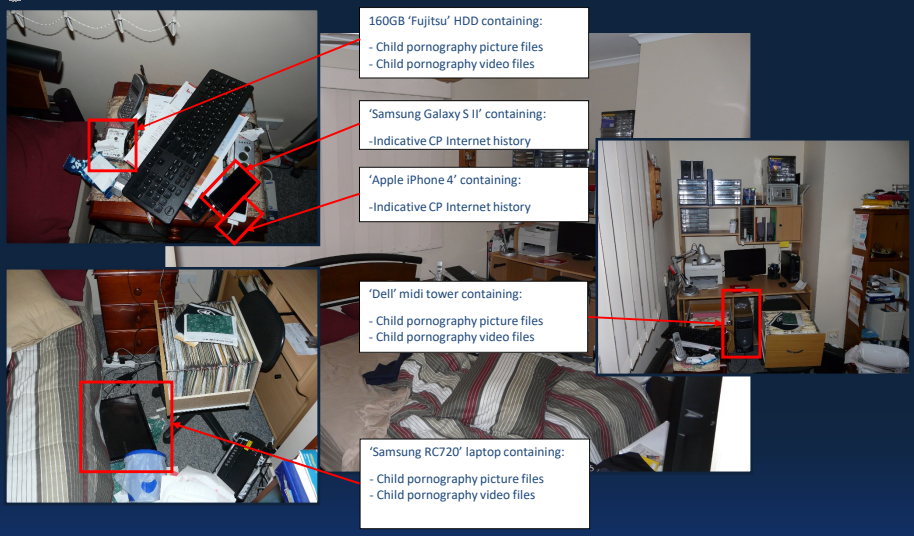
ប្រភពភស្តុតាងពីគ្រឿងអេឡិចត្រូនិច

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP AUSTRALIAN FEDERAL POLICE

ប្រភពភស្តុតាងពីគ្រឿងអេឡិចត្រូនិច



160GB 'Fujitsu' HDD containing:
- Child pornography picture files
- Child pornography video files

'Samsung Galaxy S II' containing:
-Indicative CP Internet history

'Apple iPhone 4' containing:
-Indicative CP Internet history

'Dell' midi tower containing:
- Child pornography picture files
- Child pornography video files

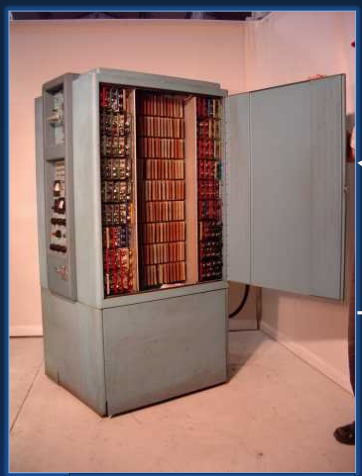
'Samsung RC720' laptop containing:
- Child pornography picture files
- Child pornography video files

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP AUSTRALIAN FEDERAL POLICE

ការប្រឈម - ទំហំទិន្នន័យ



កុំព្យូទ័រទស្សវត្តឆ្នាំ 1960s

ឯកសារនេះស្មើនឹង 10 Microsoft Word documents ដែលមានពាក្យមួយៗនៅក្នុងឯកសារនីមួយៗ

496,000+ times more storage

32GB microSD card

TRAINING-IN-CONFIDENCE

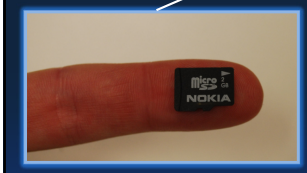
TRAINING-IN-CONFIDENCE

AFP

ការប្រឈម - ទំហំទិន្នន័យ

ដូចម្ដេច១ដើម

ក្នុងគនរសំរាម ...



MicroSD Card

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ការប្រឈម - ទំហំទិន្នន័យ

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការប្រឈម - ទំហំទិន្នន័យ

- ចំនួនទិន្នន័យដែលរឹបអូសបានៗកើនឡើងច្រើនឡើងជាលំដាប់។ 4TB HDDs អាចទទួលបាន 36+ hours នូវរូបភាព/ទាញបាន
- ស្តាកហ្គូនទំនើបមានអង្គចងចាំធំ ដែលអាចទទួលបាន ពី 2-24 hours+នៃរយៈពេលទាញរូបភាព
- ការស្រាវជ្រាវរក Keyword ឥឡូវត្រូវចំណាយពេលជាច្រើនថ្ងៃ មិនមែនច្រើនម៉ោងដូចមុនទេ
- មនុស្សឥឡូវមានកុំព្យូទ័រពហុជំនាញ និងទូរស័ព្ទចល័ត ដែលធ្វើឲ្យអ្នកស៊ើបអង្កេតចំណាយពេលវេលាច្រើនក្នុងពិនិត្យ និងវិភាគ

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការបង្ហាញឲ្យឃើញ

- **វត្ថុតាងជា USB –** ការទទួលបាន/ការផ្តុកបាន
  - USB flash memory drive exhibit
  - សារៈសំខាន់នៃដំណើរការផ្សៀងផ្ទាត់
  - ពន្យល់ និងបង្ហាញអំពី Explain hashing (with demonstration)

TRAINING-IN-CONFIDENCE

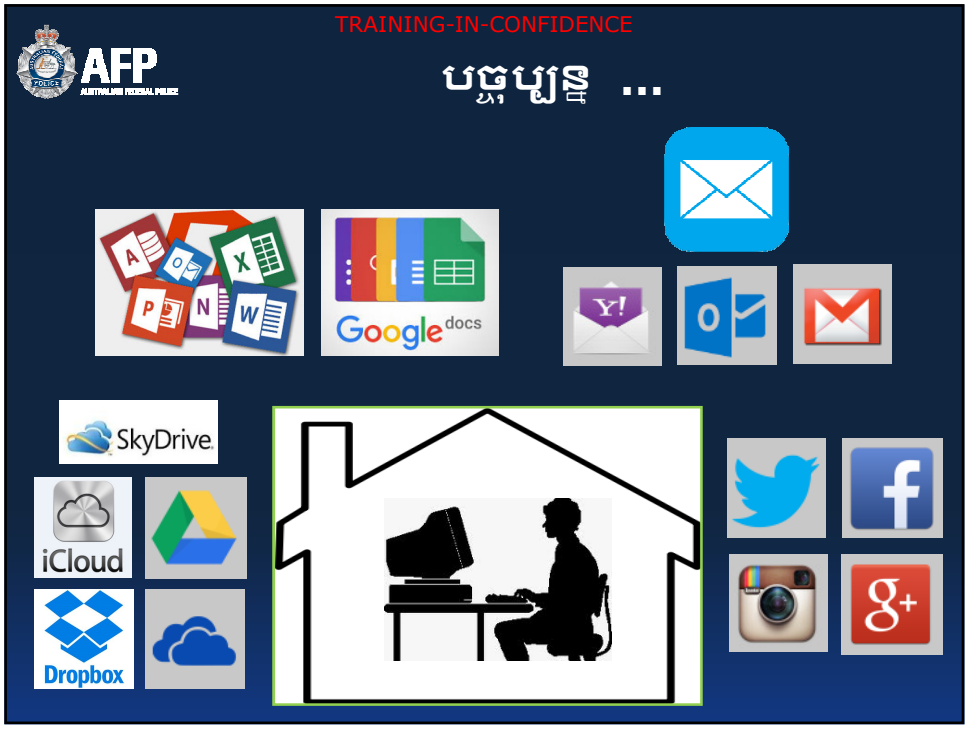
TRAINING-IN-CONFIDENCE

ការប្តូរមុខនៃកសុតាងអេឡិចត្រូនិច

TRAINING-IN-CONFIDENCE

ប្រវត្តិ

TRAINING-IN-CONFIDENCE


TRAINING-IN-CONFIDENCE
AFP
AUSTRALIAN FEDERAL POLICE
បច្ចុប្បន្ន ...
Google docs
SkyDrive
iCloud
Dropbox


TRAINING-IN-CONFIDENCE
AFP
AUSTRALIAN FEDERAL POLICE
បច្ចុប្បន្ន ...
© Google

TRAINING-IN-CONFIDENCE

ការប្រើកុំព្យូទ័រក្នុងក្លាវ (Cloud Computing)

- **ព័ត៌មានជាសារវ័ន្តមាននៅក្នុងCloud ៖**
  - ឈ្មោះអាខោន (Account names)
  - អាស័យដ្ឋាន IP addresses
  - ព័ត៌មានលម្អិតដែលបានចុះបញ្ជី (ឈ្មោះ អាស័យដ្ឋានជាដើម ។ល។)
  - ការទូទាត់លម្អិត / ឬ Credit Card details
  - មានការភ្ជាប់បណ្តាញ ឬភ្ជាប់ជាមួយអាខោនផ្សេងៗទៀត
  - បញ្ជីលេខទូរស័ព្ទទំនាក់ទំនង (Contact lists, Task lists, Friend lists)
  - Chat logs
  - Stored files
  - Emails
  - Cryptocurrency / Wallets

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

អនឡាញ ឬឧបករណ៍ចាប់យកក្នុងក្លាវ
(Online or Cloud Content Capturing Tools)

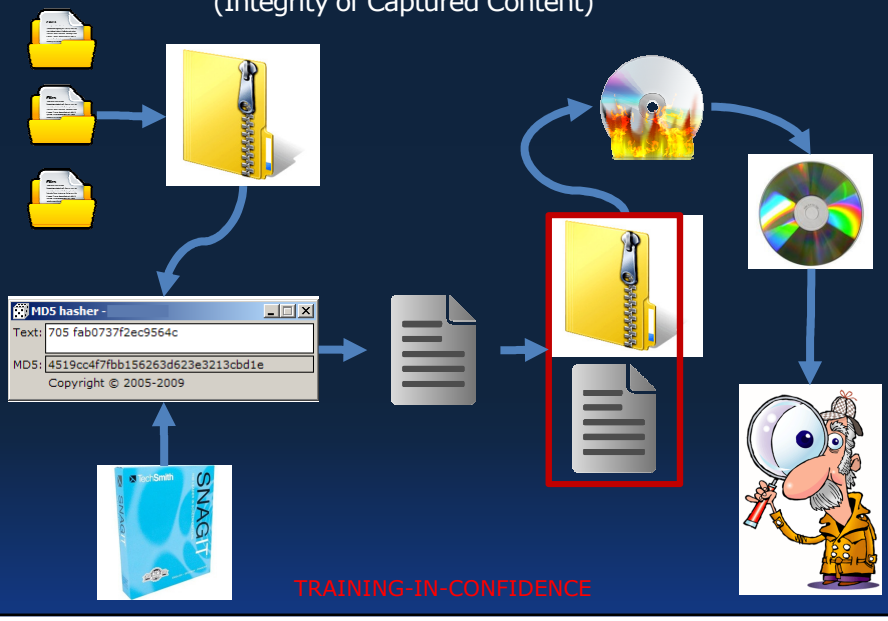
- អាចយកមកប្រើដើម្បីចាប់យកទិន្នន័យតាមអនឡាញ ឬតាមក្លាវ នៅពេលដែលយើងរក្សា/ផ្ទុកទិន្នន័យស្ត្រីន
- ឧបករណ៍សម្រាប់ចាប់តាម screen capturing, web page saving, etc:
  - Greenshot
  - FastStone Screen Capture
  - Print to PDF (PDFCreator)
  - VMWare “Capture Movie”
  - HTTrack Website Copier
  - Hunchly
  - SnagIt
  - Camtasia
  - WPS (Web Page Saver)

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ដែននៃការចាប់យកខ្លឹមសារ
(Integrity of Captured Content)



TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ការបង្ហាញឱ្យឃើញដឹង

- បច្ចេកទេសចាប់រូបលើស្ក្រីន **(Screen Capture Techniques)**
  - ការថតជារឹដេអូ ពីស្ក្រីន Screen Capture
  - ការចាប់/ថតពី web page
  - បង្កើត កន្លែងដាក់/រក្សាភស្តុតាង (Creating an Evidence Container)

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការប្រឈម - អក្សរសម្ងាត់ (Challenges – Encryption)

- មនុស្សកាន់តែច្រើនឡើងៗ ប្រើប្រាស់អក្សរសម្ងាត់
- នៅលើ Apple Macintosh, អ្នកប្រើប្រាស់បានកើនឡើង
- អក្សរសម្ងាត់នៅក្នុងទូរស័ព្ទចល័ត
- មានកម្មវិធីដូចជា VeraCrypt អាចទាញយកដោយមិនចំណាយប្រាក់ (Free) ហើយងាយស្រួល
- Advanced vendor encryption (e.g. Microsoft Office)

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការបង្ហាញឱ្យយល់ដឹង

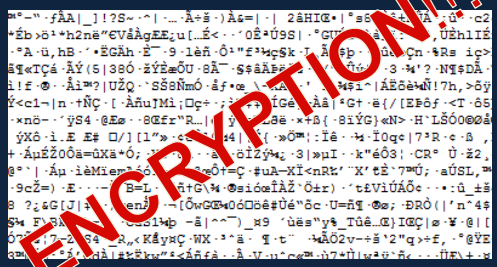
- **ការបំបែករកលេខ/អក្សរសម្ងាត់**
  (Password Cracking)
  - Windows User Account
  - Microsoft Word
  - Zip Archive

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការប្រឈម - អក្សរសម្ងាត់ (Challenges – Encryption)

- ទិន្នន័យជាលេខ ឬអក្សរសម្ងាត់ជាអ្វី?

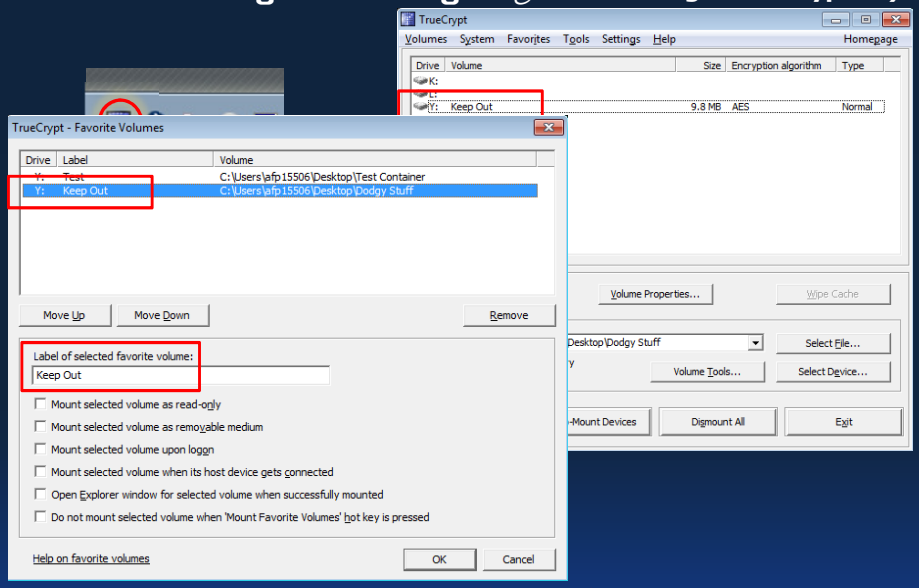


- ត្រូវការលេខសម្ងាត់ ដើម្បីចូលមើលឯកសារ/ទិន្នន័យ (password, a key, a hardware device to be decrypted and turned into a viewable file(s)
- ឧទាហរណ៍ លេខ/អក្សរសម្ងាត់នៃ file មួយគេប្រើ True/VeraCrypt

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការប្រឈម - អក្សរសម្ងាត់ (Challenges – Encryption)



TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ការប្រឈម - អក្សរសម្ងាត់ (Challenges – Encryption)

Password: "peter123"

Password: "letmein567"

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

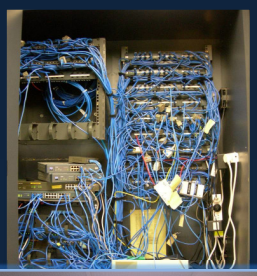
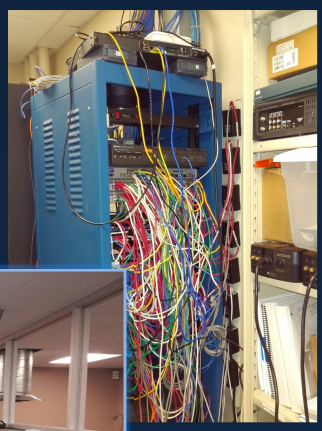
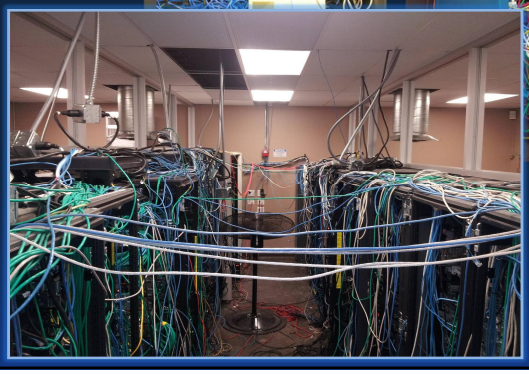
ការបង្ហាញឱ្យឃើញដឹង

- លេខ/អក្សរសម្ងាត់ប្រើ **VeraCypt**
  - បង្កើត encrypted containers
  - ការលាក់ Hidden volumes within containers (2 x passwords)
  - ការកំណត់អត្តសញ្ញាណ Identifying potential encrypted containers

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការប្រឈម - ការរៀបចំមុខងារនៃឧបករណ៍ភ្ជាប់បណ្តាញ

TRAINING-IN-CONFIDENCE

ការប្រឈម - ការរៀបចំមុខងារនៃឧបករណ៍ភ្ជាប់បណ្តាញ

- ពេលខ្លះយើងត្រូវការជំនួយពីរដ្ឋបាលកុំព្យូទ័រ
- អាចមានភាពស្មុគស្មាញ ហើយទំហំទិន្នន័យធំ
- ការរក្សាទិន្នន័យនៅខាងក្រៅ (Offsite storage is common)
- ការធ្វើកោសលវិច័យដោយផ្ទាល់គឺជាការចាំបាច់ ('Live' forensics or examinations is typically required)

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ការបង្ហាញឲ្យយល់ដឹង

- **ការធ្វើកោសលវិច័យផ្ទាល់ និង ការរក្សាកាលប្បវត្តិអាខោន** ('Live Forensics' & Archiving Accounts)
  - ទូរអង្គចងចាំ (Memory dumps) - មានសារសំខាន់ណាស់
  - Running processes
  - ការភ្ជាប់ជាមួយ USBs
  - Wi-Fi passwords
  - Gmail & Facebook Archiving

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ការធ្វើកោសលវិច័យលើទូរស័ព្ទចល័ត

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ការធ្វើកោសលវិច័យលើទូរស័ព្ទចល័ត

ខ្ញុំអាចពន្យល់អំពីការធ្វើកោសលវិច័យលើទូរស័ព្ទចល័តសម្រាប់រយៈពេលច្រើនសប្តាហ៍ក៏បាន!

ប៉ុន្តែ ខ្ញុំសុំជូនតែចំណុចសំខាន់ៗមួយចំនួនទុកជាការចងចាំ ...

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ពេលវេលាបានផ្លាស់ប្តូរជាមួយការធ្វើកោសលវិច័យចល័ត

- Gone are the days of a simple examination process:

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

បច្ចុប្បន្នវាមានភាពស្មុគស្មាញកាន់តែច្រើន...

- Encrypted handsets
- Biometrics
- Cloud storage
- Data capacity i.e. 1TB built-in storage + memory cards
- Encrypted applications
- ការលំបាកណ៏ៈ JTAG and chip-off

ឥឡូវចូរមើលលើម៉ាស៊ីន/ ឧបករណ៍របស់អ្នក

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

តើមានសុវត្ថិភាពប៉ុនណាឧបករណ៍/ម៉ាស៊ីនរបស់អ្នក?

- ENCRYPTED DEVICE MEMORY?
- ENCRYPTED MEMORY CARD?
- OPERATING SYSTEM UPDATES?
- LATEST SECURITY PATCHES?
- PASSWORD PROTECTED?
- BIOMETRIC / FACE /FINGER?
- SWIPE PIN CODE SMUDGE TEST?
- FIND MY DEVICE/iPHONE ENABLED?

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

- PHYSICAL OR LOGICAL EXTRACTION AVAILABLE?
- FILE SYSTEM EXTRACTION AVAILABLE?
- MTK BACKUP AVAILABILITY?
- ROOT / JAILBREAK AVAILABLE?
- RECOVERY PARTITION INSTALLED?
- LOCK SCREEN VULNERABILITY?
- JTAG / CHIP OFF AVAILABLE?
- CLOUD BACKUP ENABLED / PC SYNC?
- ENCRYPTED APPLICATIONS?

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

អនាគតនៃ e-SIM

TRAINING-IN-CONFIDENCE

អនាគតនៃ e-SIM

- ក្នុងរយៈពេលពីរ បីឆ្នាំខាងមុខគ្រឿងឧបករណ៍ទាំងនេះនឹងមានមុខងារដូចស៊ីមកាត ហើយមិនចាំបាច់ឲ្យក្រុមហ៊ុន Telco ផ្តល់ស៊ីមកាតឡើយ (telco issued SIM card)
- ឧបករណ៍នេះមានមុខងារដូចគ្នានឹង 'e-SIM'
- ទូរស័ព្ទ Apple iPhones ម៉ាកថ្មីប្រើ ស៊ីមពីរ dual SIMs (និង១ទៀតប្រើ e-SIM)
- Virtual SIMs នឹងអាចទាញចេញមកតាមអាកាស (will be downloaded over the air)
- អាចធ្វើឲ្យជនល្មើស ងាយស្រួលលាក់ការប្រើប្រាស់ ស៊ីម (SIM)ច្រើនមុខបាន

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ភស្តុតាងសំខាន់ៗទាក់ទងនឹងទូរស័ព្ទចល័ត

ប្រភព	អ្វីជាភស្តុតាង	បរិយាយ
ថវិកា/ទូរស័ព្ទ	**Hardware**	ទូរស័ព្ទថ្ងៃខែឆ្នាំ ពេលវេលា និង **IMEI**
	អ្នកប្រើបានបង្កើតព័ត៌មាន	**Address Book, SMS, Calendar, Calls.**
SMART Phone	អ្នកប្រើបានបង្កើតព័ត៌មាន	រូបថត វីដេអូ សម្លេង **GPS waypoints, stored voicemail, misc. files.**
	ព័ត៌មានតាមអ៊ីនធើណែត	អាខោនតាមអនឡាញ, ទិញបណ្តាញព័ត៌មាន, អ៊ីមែល ប្រើបណ្តាញអ៊ីនធើណែត បណ្តាញសង្គម
	បង្កើតភាគីទីបី **Installed 3rd Party Applications**	**Alternate messaging platforms, additional capabilities.**
កន្លែងធ្វើការ	ផ្ទេរព័ត៌មាន	**Tethered devices, back ups of handsets, back up of purchased media**

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ភស្តុតាងសំខាន់ៗទាក់ទងនឹងទូរស័ព្ទចល័ត

ប្រភព	អ្វីជាភស្តុតាង	បរិយាយ
Carrier	**Tracking Information**	**Connected cell towers, location of handset.**
	Usage Information	**Billing Information; call registers; internet/data usage; messages not delivered.**
SIM Card	**Identifiers**	**Subscriber identifier (IMSI); SIM card identifier (ICC-ID)**
SIM Card	**Usage Information**	**SMS; Address book, last dialed numbers; last cell tower;**

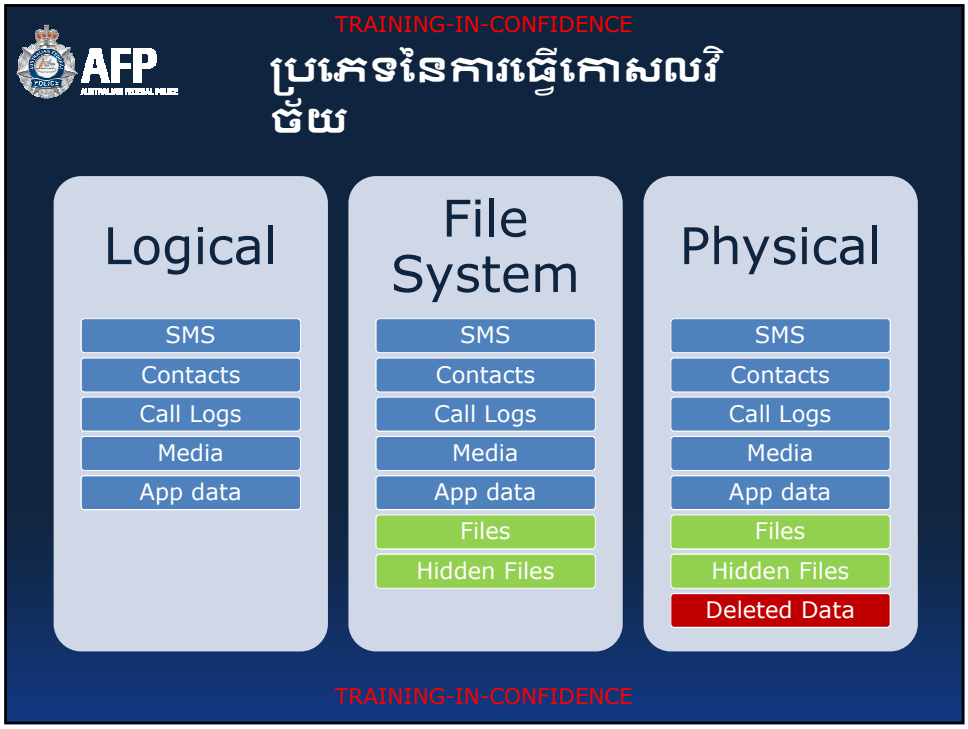
TRAINING-IN-CONFIDENCE

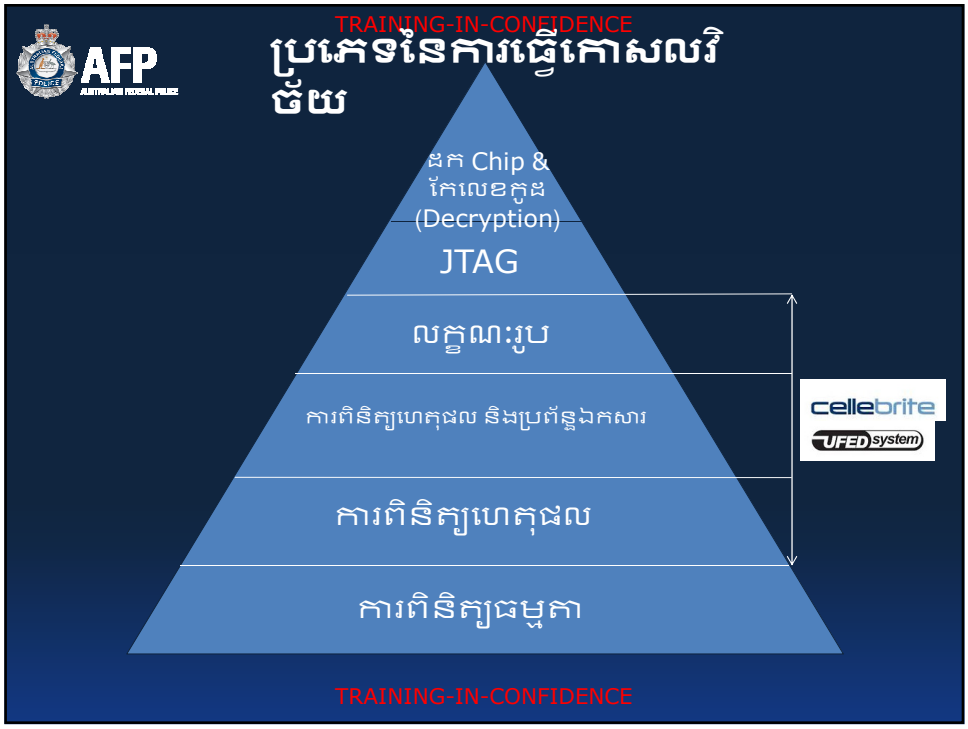
TRAINING-IN-CONFIDENCE

ប្រភេទដែលទាញយកព័ត៌មានពីទូរស័ព្ទ

- ការថតចម្លងយក **logical extraction** copies **user data** ពីកន្លែងដែលរក្សាទិន្នន័យ
- ការទាញយកឯកសារពីប្រព័ន្ធ **file system extraction** copies **user and system data** ពីកន្លែងដែលរក្សាទិន្នន័យ
- ការទាញយក **physical extraction** ដែលមានការថតទិន្នន័យពី device's storage media, **including deleted data** (closest to a forensic 'bit for bit' image).
- ការទាញយកតាមបែប logical extraction អាចលឿនជាង physical extraction
- គ្រឿងឧបករណ៍ខ្លះមិនអាចទាញតាម **physically extracted**.
- Logical extractions **may recover some deleted data** depending on the phone and operating system version.

TRAINING-IN-CONFIDENCE


TRAINING-IN-CONFIDENCE
AFP
ប្រភេទនៃការធ្វើកោសលវិច័យ
Logical
SMS
Contacts
Call Logs
Media
App data
File System
SMS
Contacts
Call Logs
Media
App data
Files
Hidden Files
Physical
SMS
Contacts
Call Logs
Media
App data
Files
Hidden Files
Deleted Data
TRAINING-IN-CONFIDENCE


TRAINING-IN-CONFIDENCE
AFP
ប្រភេទនៃការធ្វើកោសលវិច័យ
ដក Chip & កែលេខកូដ (Decryption)
JTAG
លក្ខណៈរូប
ការពិនិត្យហេតុផល និងប្រព័ន្ធឯកសារ
ការពិនិត្យហេតុផល
ការពិនិត្យធម្មតា
cellebrite
UFED system
TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ការបង្ហាញឲ្យយល់ដឹង

- ការទាញយកព័ត៌មានចេញពីទូរស័ព្ទចល័ត (ដៃ)
  - ការទាញយកព័ត៌មានដោយប្រើ Cellebrite UFED 4PC
  - ការពិនិត្យមើលទិន្នន័យក្នុង Cellebrite Physical Analyzer

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

ច្បាប់ទាក់ទងនឹងការធ្វើកោសលវិច័យតាមឌីជីថុល

- ច្បាប់ព្រហ្មទណ្ឌ (Crimes Act 1914)
  - អំពីភស្តុតាងអេឡិចត្រូនិច្ចនៅជំពូកមុនគេ គឺនៅ Sections 3K – 3Z
- ច្បាប់ទាក់ទងនឹងការធ្វើកោសលវិច័យឌីជីថុល Digital Forensics:
  - នៅក្នុងចំណុច 3K – the '14-day Provision'
  - នៅក្នុងចំណុច 3L(1) – ការប្រតិបត្តិការឧបករណ៍អេឡិចត្រូនិច្ចនៅក្នុងបរិវេណ/កន្លែង
  - នៅក្នុងចំណុច 3LA – compel POI to provide information or assist
  - នៅក្នុងចំណុច 3ZQV – ឧបករណ៍អេឡិចត្រូនិច្ចអាចយកមកប្រតិបត្តិការវិញបានបន្ទាប់ពីការរឹបអូស ឬដកហូត

ខ្ញុំនឹងពន្យល់អំពីគោលការណ៍ទាំងនេះឲ្យបានលម្អិត

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការមកទស្សនកិច្ចនៅកម្ពុជាថ្មីៗ

នៅថ្ងៃទី **3-7** ខែ **មិថុនា** ឆ្នាំ **2019**

- ការបណ្តុះបណ្តាលការធ្វើកោសលវិច័យឌីជីថុល DF និង Cellebrite UFED:
  - ដីកាឆែកឆេរ – triaging of devices
  - Write-protection and forensic integrity of evidence
  - ស្តង់ដានីតិវិធីវិប្រតិបត្តិការ និង SOP and BPGs
  - បច្ចេកទេសចាប់យក
  - ឧបករណ៍វិភាគ
  - ធ្វើកោសលវិច័យទូរស័ព្ទចល័តដោយប្រើ Cellebrite UFED

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការមកទស្សនកិច្ចនៅកម្ពុជាថ្មីៗ

នៅថ្ងៃទី **3-9 ខែមេសា** ឆ្នាំ **2019**

- មានការស្នើសុំឲ្យផ្តែកកោសលវិច័យឌីជីថុលរបស់ AFP ដើម្បីជួយធ្វើការស៊ើបអង្កេតលើករណីអាជីវកម្មផ្លូវភេទលើកុមារ
- រៀបចំដោយ នាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិជ្ជានៃនគរបាលជាតិកម្ពុជា
- មានឧបករណ៍អេឡិចត្រូនិច្ច១៥គ្រឿង មានផ្ទុកព័ត៌មានយ៉ាងច្រើនដែលត្រូវទាញយកក្នុងរយៈខ្លី
- AFP ត្រូវការ Copy នូវព័ត៌មានពីឧបករណ៍អេឡិចត្រូនិច្ចទាំងអស់ដើម្បីធ្វើការស៊ើបអង្កេតបន្ថែម
- បង្កើនការយល់ដឹងនូវសមត្ថភាពកោសលវិច័យឌីជីថុលរបស់នគរបាលកម្ពុជាចំពោះបញ្ហាដែលពួកគេជួបប្រទះបច្ចុប្បន្ន
- ការធ្វើកោសលវិច័យឌីជីថុលរបស់នគរបាលកម្ពុជាមានទិសដៅដូចគ្នាទៅនឹងតួនាទីនៃការធ្វើកោសលវិច័យឌីជីថុលរបស់នគរសហព័ន្ធអូស្ត្រាលីដែរ

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

តើការធ្វើកោសលវិច័យឌីជីថុលរបស់នគរបាលកម្ពុជា អាចជួយអ្វីខ្លះដល់ការស៊ើបអង្កេតរបស់អ្នក?

- ការធ្វើកោសលវិច័យឌីជីថុលគឺជាការងារជំនាញដែលអ្នកអាច៖
  - ពន្យល់អំពីគោលការបច្ចេកទេស
  - ផ្តល់គោលការណែនាំស្តីពីភស្តុតាងអេឡិចត្រូនិច
  - ជួយនៅពេលមានដីកាឆែកឆេរ ឧទាហរណ៍៖ របៀប Triaging of items
  - ប្រើប្រាស់ "ការអនុវត្តន៍ល្អប្រសើរ" 'best practices' ដើម្បីធានាប្រសិទ្ធិភាពនៃភស្តុតាងពីការធ្វើកោសលវិច័យសម្រាប់ផ្តល់ឲ្យតុលាការ

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការធ្វើកោសលវិច័យឌីជីថុលរបស់នគរបាលជាតិកម្ពុជា

- ការធ្វើកោសលវិច័យឌីជីថុលធ្វើឲ្យយើងដឹងអំពី៖
  - សារៈសំខាន់នៃការកត់ត្រារាល់ឯកសារ នៅមុនពេល ក្នុងអំឡុងពេល និងក្រោយពេលដំណើរពិនិត្យឧបករណ៍អេឡិចត្រូនិច
  - ផលិតចេញជាកំណត់ហេតុនៃករណី ទាញបានរូបភាព ទាញបានសកម្មភាព/ ជាដំហ៊ានពីការធ្វើកោសលវិច័យ
  - ធានាថានីតិវិធីនៃការឃុំឃាំងត្រូវបានគោរពតាម

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការធ្វើកោសលវិច័យឌីជីថុលរបស់នគរបាលជាតិកម្ពុជាអាចជួយដល់សំណួរត្រួតពិនិត្យសំខាន់ៗនៅពេលអនុវត្តដីកាឆែកឆេរ ក្នុងនោះមាន៖

- តើឧបករណ៍នោះនៅដំណើរការ/បើកឬទេ?
- តើមានអ្វីកើតឡើង/យ៉ាងម៉ិចដែរប្រសិនបើឧបករណ៍នោះត្រូវបានបិទនៅឯកន្លែងកើតហេតុ?
- តើអ្នកត្រូវធ្វើដូចម្តេចជាមួយ Password និងលេខកូដ/ពាក្យសម្ងាត់ផ្សេងៗទៀតក្នុងឧបករណ៍?
- តើអ្នកត្រូវធ្វើដូចម្តេចដើម្បីឲ្យហ្វូននោះដាច់ចេញពីបណ្តាញ (network)?

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ការធ្វើ Triaging នៅកន្លែងកើតហេតុតាមដីការឆែកឆេរ?

- នគរបាល AFP ចូលរួមគ្រប់ដីកាឆែកឆេរលើករណីអាជីវកម្មផ្លូវភេទលើកុមារ
- ការធ្វើ Triaging (ការពិនិត្យជាមុន) ពិនិត្យឧបករណ៍តាមដីកាឆែកឆេរអាចជួយការស៊ើបអង្កេតបានច្រើនយ៉ាង ដូចជា៖
  - ការរកឃើញភស្តុតាងនៅនឹងកន្លែងផ្ទាល់អាចនាំទៅដល់ការសារភាពភ្លាមៗ
  - ទាញយកបាននូវ "ទិន្នន័យផ្សាយផ្ទាល់" 'live' data" នៅលើឧបករណ៍ដែលកំពុងដំណើរការកូដសម្ងាត់
  - បន្ថយការប្រមូល/រឹបអូសឧបករណ៍ ហេតុដូច្នេះហើយអាចបន្តយការពិនិត្យនៅមន្ទីរពិសោធន៍
  - អាចទាញបាន រក្សាទុក មានអាខោនអនឡាណ ឧទា. អាខោន Facebook និង Gmail
  - រក្សាទូរស័ព្ទនោះឲ្យដាច់ចេញពីបណ្តាញ (Network)
  - ជានាសំណុំទិន្នន័យនៅក្នុងឧបករណ៍

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

ដំណាក់កាលពិនិត្យឡើងវិញនៃដំណើរការកោសលវិច័យឌីជីថុល៖

- ការធ្វើអត្តសញ្ញាណកម្ម និងការរឹបអូស
- ការទទួលបាន
- ការវិភាគ
- ការរាយការណ៍

តើយើងត្រូវចែកដំណាក់កាល/ បំណែកៗយ៉ាងដូចម្តេចដើម្បីបង្ហាញតុលាការ?

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

និងសេវាកោសលវិច័យឌីជីថុល និងរបាយការណ៍របស់ AFP

- សេចក្តីថ្លែងអំពីការធ្វើកោសលវិច័យឌីជីថុល៖
  - ក្រាប់ឈ្មោះអ្នកពិនិត្យ និងរបាយការណ៍
- របាយការណ៍កោសលវិច័យឌីជីថុល៖
  - បានចូលរួមតាមដីកាឆែកឆេរ
  - ខ្សែសង្វាក់នៃការឃុំឃាំង (Chain of Custody)
  - ការសន្និដ្ឋាន (Assumptions) , ការកម្រិត និងដំណើរការ/នីតិវិធី
  - ការសង្ខេបអំពីការធ្វើកោសលវិច័យ/ការពិនិត្យ
  - រៀបរាប់អំពីឧបករណ៍ភស្តុតាង និងការវិភាគអ្វីដែលបានរកឃើញ

ខាងក្រោមនេះជាឧទាហរណ៍ខ្លះ ...

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP រង្វាន់ចុងក្រោយសម្រាប់ការស៊ើបអង្កេតរបស់អ្នក

- បទល្មើសឧក្រិដ្ឋអាចកើតចេញពីបច្ចេកវិជ្ជា (cyber-enabled crimes) (ឧទា. បញ្ហាអាជីវកម្មផ្លូវភេទលើកុមារ), ការធ្វើកោសលវិច័យឌីជីថុលមានសារៈសំខាន់បំផុត៖
- ចូលរួមការធ្វើកោសលវិច័យនៅដំណាក់កាលដំបូងក្នុងការស៊ើបអង្កេតលើឧបករណ៍តាមគោលការបច្ចេកទេសដូចជា VPNs, និងគោលការអនុវត្តន៍ល្អប្រសើរ បញ្ហាលេខកូដ/អក្សរសម្ងាត់ អំពីបញ្ហាទូរស័ព្ទចល័ត ។ល។
- អ្នកត្រូវតែព្យាយាមប្រើការធ្វើកោសលវិច័យនៅពេលមានដីកាឆែកឆេរមើល triaging of devices, និងចាប់/ប្រមូលយកឲ្យបានត្រឹមត្រូវទិន្នន័យបន្តផ្ទាល់នៅកន្លែងកើតហេតុ ទាញយកមកវិភាគទុកអាខោនអនឡាន ។ល។

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP រង្វាន់ចុងក្រោយសម្រាប់ការស៊ើបអង្កេតរបស់អ្នក

- រៀបចំកម្មវិធីប្រជុំឲ្យបានទៀងទាត់ជាមួយ CNP DF ដើម្បីពិភាក្សាអំពីបញ្ហាបច្ចុប្បន្ន អំពីនិន្នាការ អំពីការយល់ដឹងនូវចំណេះដឹងបច្ចេកទេសថ្មីៗ និងកម្មវិធី software ជាដើម

- ចំណាំ ៖ CNP DF គឺជាជំនាញឯកទេសរបស់អ្នក ជំនាញទាំងនោះអាចជួយដោះស្រាយអ្នក មុនហេតុការណ៍ ក្នុងហេតុការណ៍ និងក្រោយហេតុការណ៍

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

បន្តទទួលយកចំណេះដឹងបច្ចេកទេសស៊ើបអង្កេតថ្មី សម្រាប់បង្កើនកម្រិតចំណេះដឹងថ្មីទៀត!

- បង្កើនមូលដ្ឋានចំណេះដឹង និងជំនាញរបស់អ្នក
- ការធ្វើកោសលវិច័យឌីជីថល ការឆ្លើយតបឧបទ្ទវហេតុ, ការវិភាគ, លេខកូដ/អក្សរសម្ងាត់ ។ល។ គឺជាផ្នែកឯកទេសដែលតែងតែមានការផ្លាស់ប្តូរ
- ប្រសិនបើអ្នកជាអ្នកកោសលវិច័យឌីជីថល ជាអ្នកស៊ើបអង្កេត ឬជាព្រះរាជអាជ្ញា អ្នកគួរព្យាយាមដើម្បីឲ្យខ្លួនឯងមានចំណេះដឹង/ចេះប្រើនូវឧបករណ៍ វេទិកា វិញ្ញាបនប័ត្រមួយចំនួនតាមរយៈ ....

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

- **CompTIA** (https://www.comptia.org) provides a fundamental knowledge base
  - A+, Network+, Security+
- International Society of Forensic Computer Examiners (https://www.isfce.com) – certification and forum
- International Association of Computer Investigative Specialists (https://www.iacis.com) – cert and forum
- Be comfortable with different operating systems
  - **Computers:** Windows, Mac OS, Linux
  - **Phones:** Android, iOS, Windows

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP

- **SANS** (https://www.sans.org)
  - Various certifications
  - DFIR SIFT Workstation
- **Kali Linux** – Ethical hacking
- USB Forensic Bootable Environments:
  - Paladin
  - Caine
  - Linux Tails – Anonymous activity on Dark Web
- **SWGDE** (https://www.swgde.org) – workflows, best practice guides, etc

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE

ការបញ្ចប់ការគិត

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE

តើមានសំណួរអ្វី ចុងក្រោយដែរឬទេ?

TRAINING-IN-CONFIDENCE

TRAINING-IN-CONFIDENCE

AFP
AUSTRALIAN FEDERAL POLICE

សូមអរគុណដ៏ជ្រាលជ្រៅចំពោះ ការយកចិត្តទុកដាក់ស្តាប់

TRAINING-IN-CONFIDENCE