COMBITECH

Michael Johansson
Alexander Rautenberg

LNU 2019

GUEST LECTURE: FORENSICS

WHOAMI

- Michael Johansson
  - 29 years old
  - In the security 6ish år
  - Studied 3 years at LNU (Network security 2015-2018)

  - Any IT/Security questions, contact me @
    - Michael.johansson@combitech.se
    - +46734 37 61 69

COMBITECH

WHAT ARE COMBITECH

Combitech

- Located in different locations around Sweden
- 1800 ish employees
- IT security/Penetration testing/Incident Response/Secure code

- Incident Response for the whole SAAB, Austrailia, India, Brasil etc
- Incident Response for Private/public sector as well.
- Almost never any civil cases.

Saab

50 000 incidents a day (World wide)
100ish need active investigation
1ish major incident a day

COMBITECH

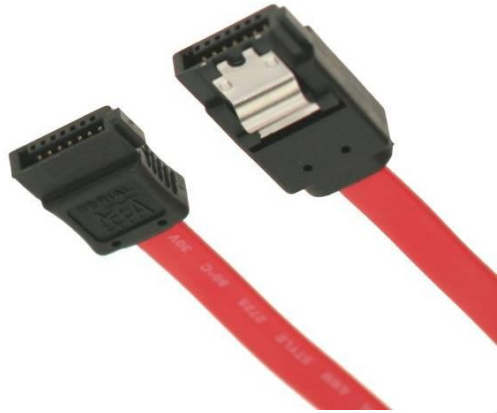
COMPUTER FORENSICS

Tools

- Disc duplicators
- Write blockers
- Adapters
- Cameras

Requirements

- Disk drives
- Cables
- USB storage devices



COMBITECH

COMPUTER FORENSICS - DUPLICATOR

Disc Duplicators

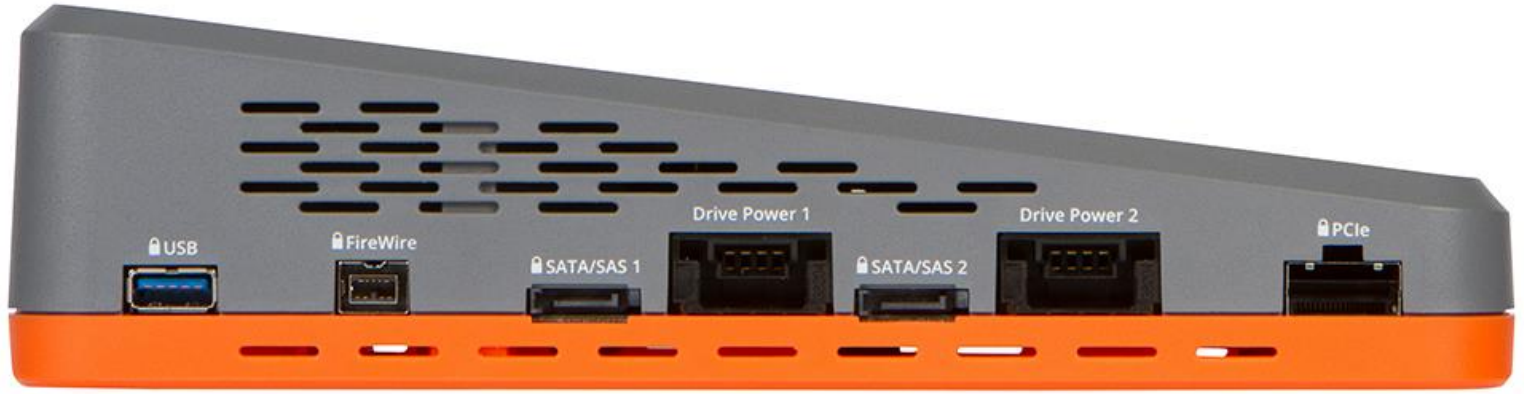
- How it works
  - Clones entire devices to various formats
    - E01 and Ex1 files (compressed images)
    - Exact copy
    - …

COMBITECH

COMPUTER FORENSICS - DUPLICATOR

Disc Duplicators

- How it works
  - One side is write blocked (EVIDENCE SIDE)
  - One side is writable (CLONE SIDE)
- Read/Write different media
  - Hard drives
  - USB
  - Network



COMBITECH

COMPUTER FORENSICS – WRITE BLOCKERS

Write blockers

Fast browsing of media

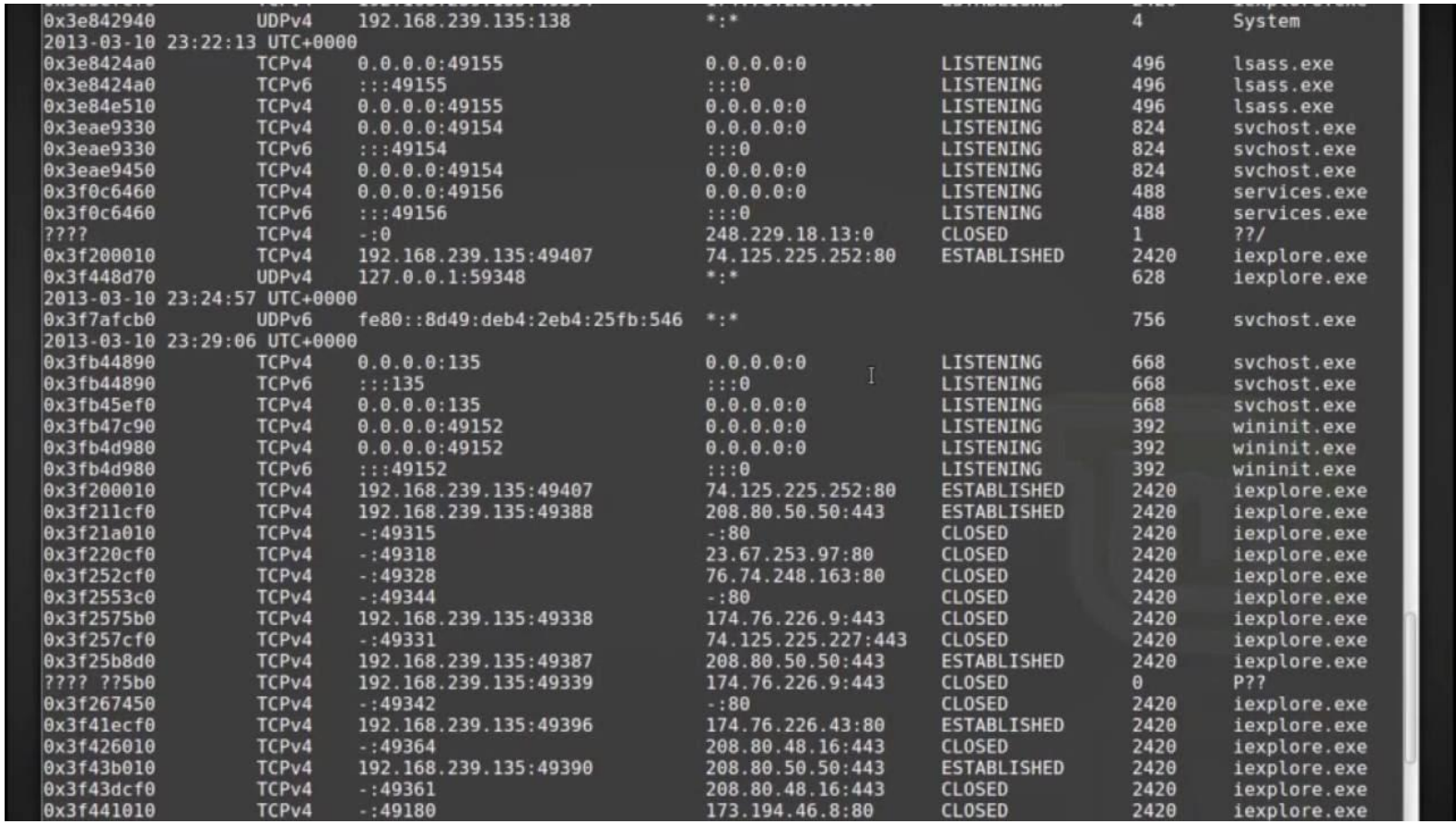
- How it works
  - One side is write blocked (EVIDENCE SIDE)
  - One side is accessed from computer
- Many different blockers
  - SATA
  - USB
  - Fire wire
  - IDE
  - SCSI
  - …

COMBITECH

COMPUTER FORENSICS – LIVE FORENSICS

Why Live Forensics

- Detect disk encryption
- Identify running processes
- Identify active communications
- Extract volatile data
- Extract from running system
  - FTK Imager
  - Mac – time capsule?
  - Linux – dd (disk duplicate)
- …



```
0x3e842940         UDPv4    192.168.239.135:138            *:*                                    4       System
2013-03-10 23:22:13 UTC+0000
0x3e8424a0         TCPv4    0.0.0.0:49155                  0.0.0.0:0              LISTENING       496     lsass.exe
0x3e8424a0         TCPv6    :::49155                       :::0                   LISTENING       496     lsass.exe
0x3e84e510         TCPv4    0.0.0.0:49155                  0.0.0.0:0              LISTENING       496     lsass.exe
0x3eae9330         TCPv4    0.0.0.0:49154                  0.0.0.0:0              LISTENING       824     svchost.exe
0x3eae9330         TCPv6    :::49154                       :::0                   LISTENING       824     svchost.exe
0x3eae9450         TCPv4    0.0.0.0:49154                  0.0.0.0:0              LISTENING       824     svchost.exe
0x3f0c6460         TCPv4    0.0.0.0:49156                  0.0.0.0:0              LISTENING       488     services.exe
0x3f0c6460         TCPv6    :::49156                       :::0                   LISTENING       488     services.exe
????               TCPv4    -:0                            248.229.18.13:0        CLOSED          1       ??/
0x3f200010         TCPv4    192.168.239.135:49407          74.125.225.252:80      ESTABLISHED     2420    iexplore.exe
0x3f448d70         UDPv4    127.0.0.1:59348                *:*                                    628     iexplore.exe
2013-03-10 23:24:57 UTC+0000
0x3f7afcb0         UDPv6    fe80::8d49:deb4:2eb4:25fb:546  *:*                                    756     svchost.exe
2013-03-10 23:29:06 UTC+0000
0x3fb44890         TCPv4    0.0.0.0:135                    0.0.0.0:0              LISTENING       668     svchost.exe
0x3fb44890         TCPv6    :::135                         :::0                   LISTENING       668     svchost.exe
0x3fb45ef0         TCPv4    0.0.0.0:135                    0.0.0.0:0              LISTENING       668     svchost.exe
0x3fb47c90         TCPv4    0.0.0.0:49152                  0.0.0.0:0              LISTENING       392     wininit.exe
0x3fb4d980         TCPv4    0.0.0.0:49152                  0.0.0.0:0              LISTENING       392     wininit.exe
0x3fb4d980         TCPv6    :::49152                       :::0                   LISTENING       392     wininit.exe
0x3f200010         TCPv4    192.168.239.135:49407          74.125.225.252:80      ESTABLISHED     2420    iexplore.exe
0x3f211cf0         TCPv4    192.168.239.135:49388          208.80.50.50:443       ESTABLISHED     2420    iexplore.exe
0x3f21a010         TCPv4    -:49315                        -:80                   CLOSED          2420    iexplore.exe
0x3f220cf0         TCPv4    -:49318                        23.67.253.97:80        CLOSED          2420    iexplore.exe
0x3f252cf0         TCPv4    -:49328                        76.74.248.163:80       CLOSED          2420    iexplore.exe
0x3f2553c0         TCPv4    -:49344                        -:80                   CLOSED          2420    iexplore.exe
0x3f2575b0         TCPv4    192.168.239.135:49338          174.76.226.9:443       CLOSED          2420    iexplore.exe
0x3f257cf0         TCPv4    -:49331                        74.125.225.227:443     CLOSED          2420    iexplore.exe
0x3f25b8d0         TCPv4    192.168.239.135:49387          208.80.50.50:443       ESTABLISHED     2420    iexplore.exe
???? ??5b0         TCPv4    192.168.239.135:49339          174.76.226.9:443       CLOSED          0       P??
0x3f267450         TCPv4    -:49342                        -:80                   CLOSED          2420    iexplore.exe
0x3f41ecf0         TCPv4    192.168.239.135:49396          174.76.226.43:80       ESTABLISHED     2420    iexplore.exe
0x3f426010         TCPv4    -:49364                        208.80.48.16:443       CLOSED          2420    iexplore.exe
0x3f43b010         TCPv4    192.168.239.135:49390          208.80.50.50:443       ESTABLISHED     2420    iexplore.exe
0x3f43dcf0         TCPv4    -:49361                        208.80.48.16:443       CLOSED          2420    iexplore.exe
0x3f441010         TCPv4    -:49180                        173.194.46.8:80        CLOSED          2420    iexplore.exe
```

COMBITECH

COMPUTER FORENSICS - EVIDENCE

Evidence

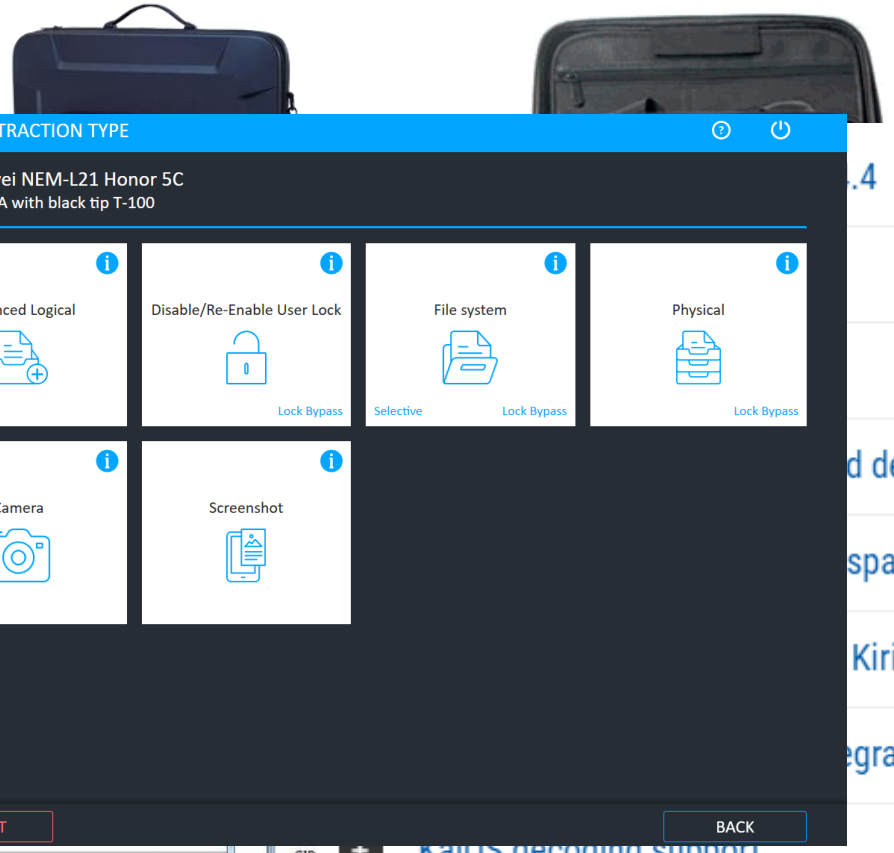
- **Communications**
- **Web history**
- **Files and documents**
- **Passwords**
- **Malware**
- **…**

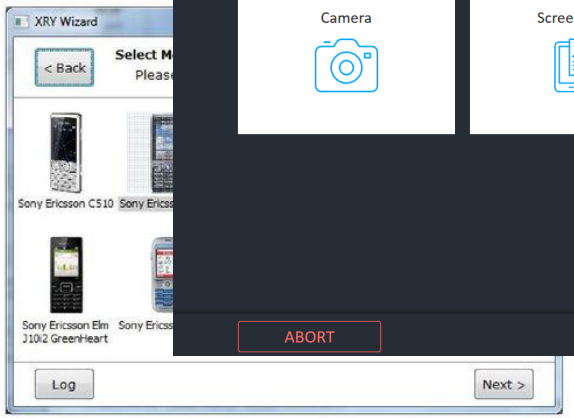
COMBITECH

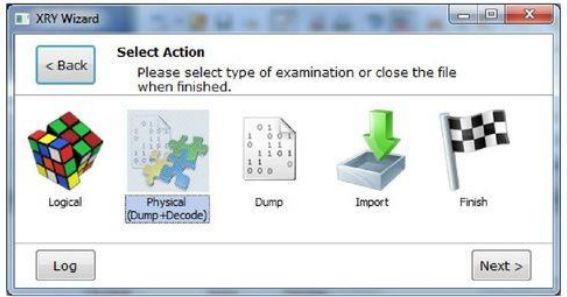
MOBILE FORENSICS - XRY

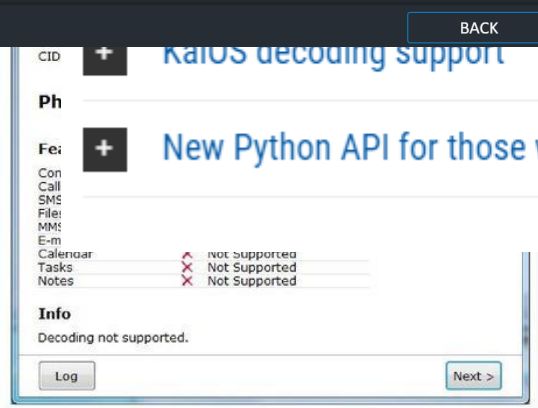
Unlock and retrieve

- How it works
  - Can use exploits to unlock
  - Retrieves data from all* devices
- Different devices
  - Cables & adapters
  - How-to checklist
- Analysis program is free
- Extraction tool is licensed







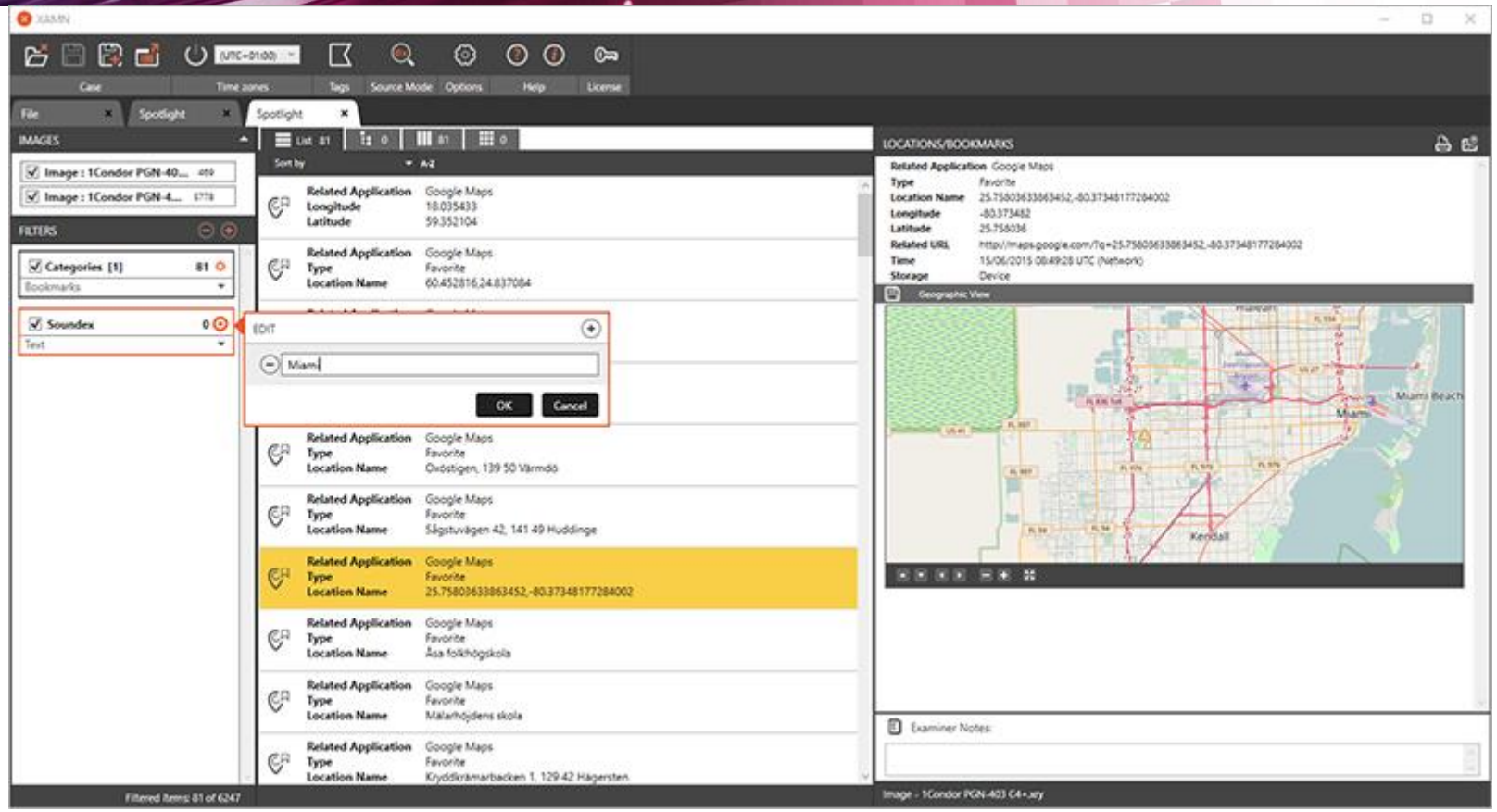


COMBITECH

MOBILE FORENSICS - XRY

What we find

- Contacts
- GEO Data
  - Photos
  - Tracking software
  - GPS
- Communications
- Web history
- …



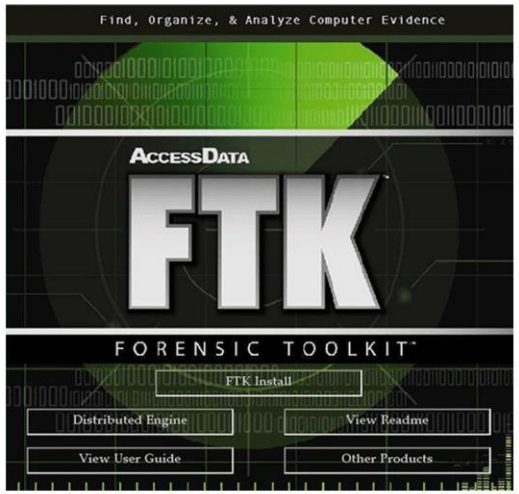
COMBITECH

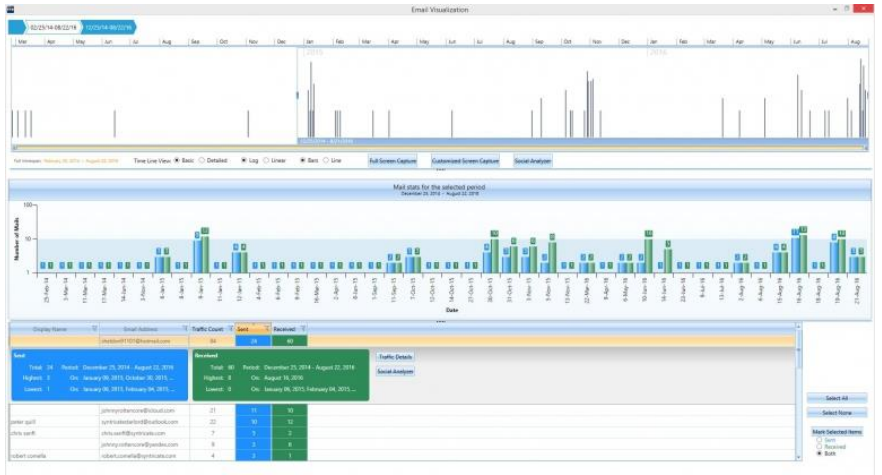
FORENSIC ANALYSIS - PROGRAMS

We use primarily

- **FTK**
- **XRY**

- **Great for education**
- **Autopsy Forensic suite**





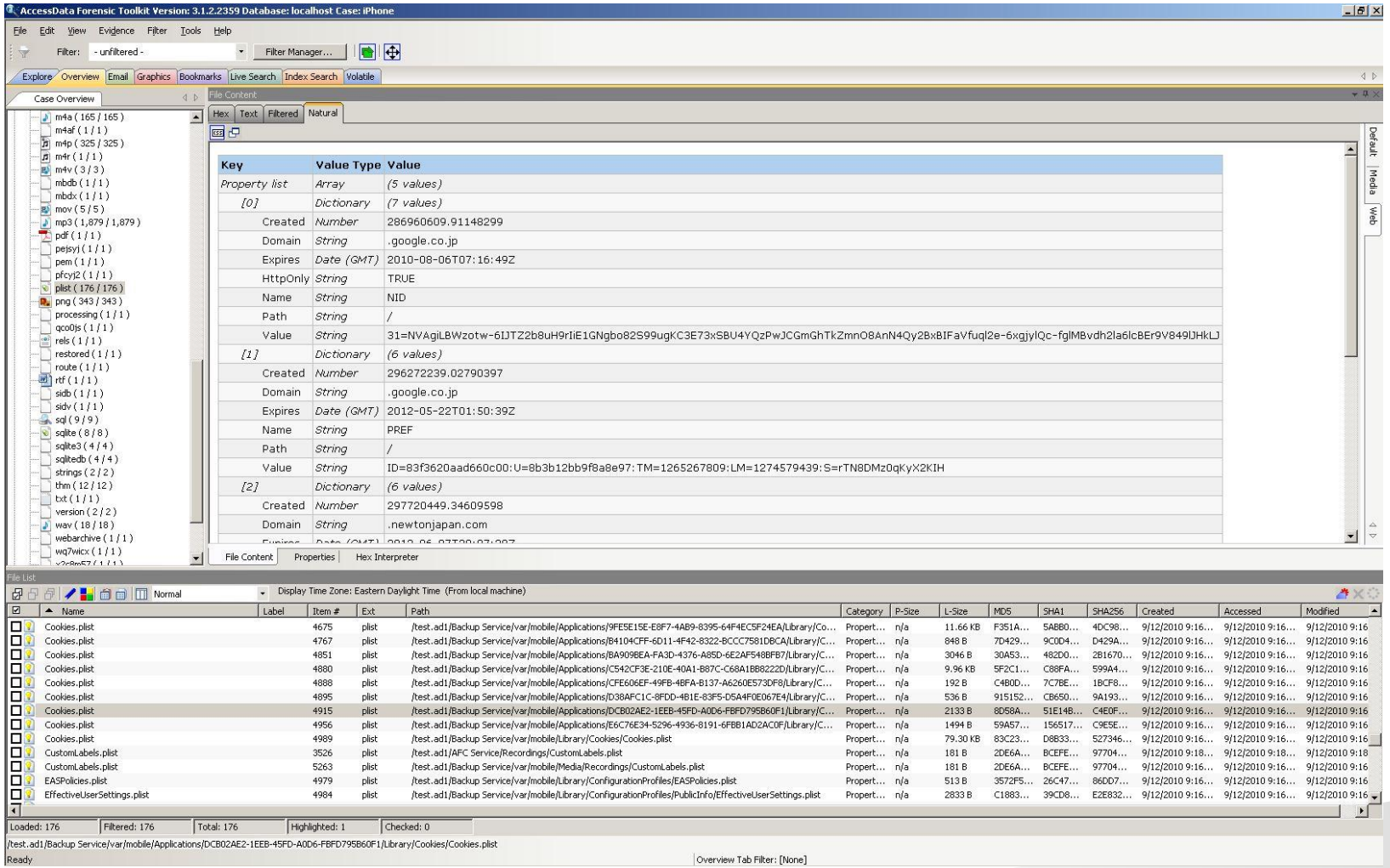
Autopsy®
OPEN | EXTENSIBLE | FAST

COMBITECH

FORENSIC ANALYSIS - PROGRAMS

How they work

- Index files
- Extract useful data
- Find deleted
- Identify file type
- View all* files
- Build time lines
- Tag Evidence
- Create report from Evidence



COMBITECH

SCENARIO 1 (NORWAY)

- Bank
  - Supply chain
  - Black mail
  - Loss of personal data
  - Fired
  - Black listed from financial jobs

COMBITECH

SCENARIO 2 (BRAZIL)

- Industry
  - Spionage
  - Multi miljon dollar loss in RnD.
  - Security issue
  - Never caught
  - Insider?
  - APT?

COMBITECH

SCENARIO 3 (SWEDEN)

- Industry
  - Insider
  - Consultant
  - Not from sweden
  - Caught with USBs containing malware
  - No indication of compromise

COMBITECH

Questions?

Else let's touch some hardware!

COMBITECH

Michael.Johansson@combitech.se

+46 734 27 61 69