

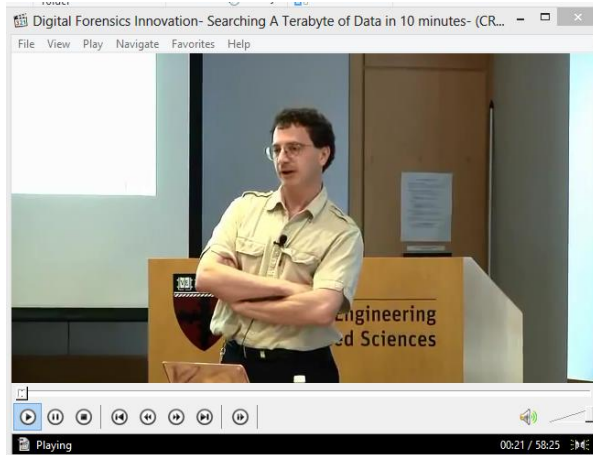
**Keamanan Jaringan Komputer
Digital Forensic**



**Disusun Oleh :
Nama : Imam Mustofa
NIM : 09011181320028**

**SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017**

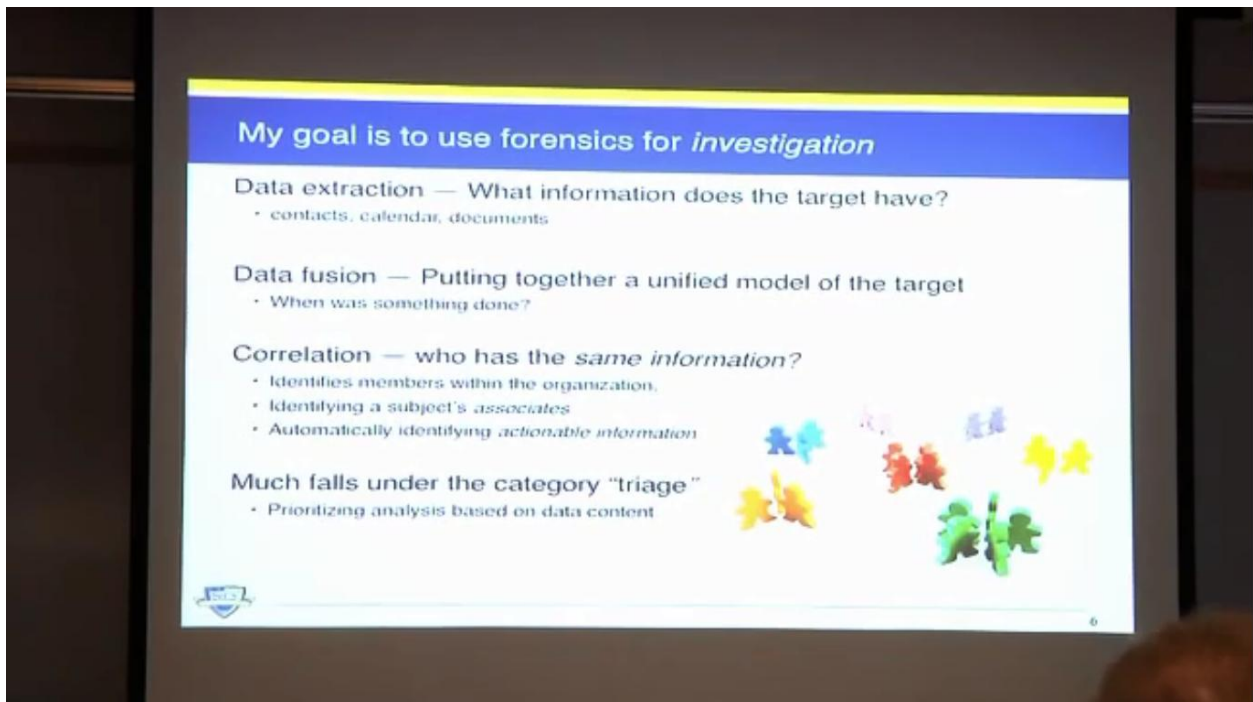
Informasi yang dibawakan oleh pembicara dibawah ini adalah sebuah terobosan inovasi dalam pengambilan data dengan kecepatan tinggi terhadap data-data forensic.



Pada tampilan slide diatas yang merupakan perjalanan identitas dari pembicara.



Yang dijelaskan pertama kali dalam presentasi yang dilakukan adalah mengenai digital forensic mulai dari caranya yang tradisional kepada sesuatu hal



Pembicara menerangkan penggunaan dari forensic yang dikhususkan kepada investigasi dengan berbagai hal yang menyangkut pada pengolahan data sesuai dengan tujuan.

Given sufficient data, we can automatically assemble complex social network diagrams

We analyzed 2000 hard drives.

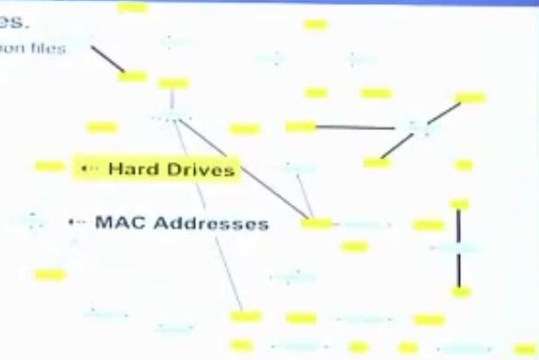
- Find IP packets in swap & hibernation files
- Extract ethernet MAC addresses.

Post-processing identifies:

- Shared wireless routers.
- Common ethernet routers.

Validation:

- Reconstructed networks came from same organization



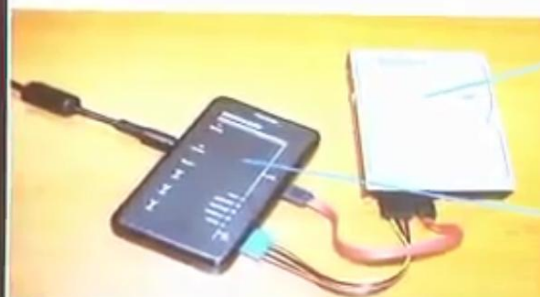
— *Forensic Carving of Network Packets and Associated Data Structures, Beverly & Garfinkel, DFRWS 2011, August 2011, New Orleans*

8


Pembicara menerangkan proses pengolahan data dengan jumlah dan criteria yang diinginkan sehingga membentuk diagram tersendiri, yang ditekankan pada slide diatas bahwa setiap pengiriman data akan mendapatkan mac address dari dua hal yaitu komputer sumber dan dari router.

Data extraction is the first step of forensic analysis


"Imaging tools" extract the data without modification.



"Write Blocker" prevents accidental overwriting.



Forensic copy ("disk image") stored on a storage array.

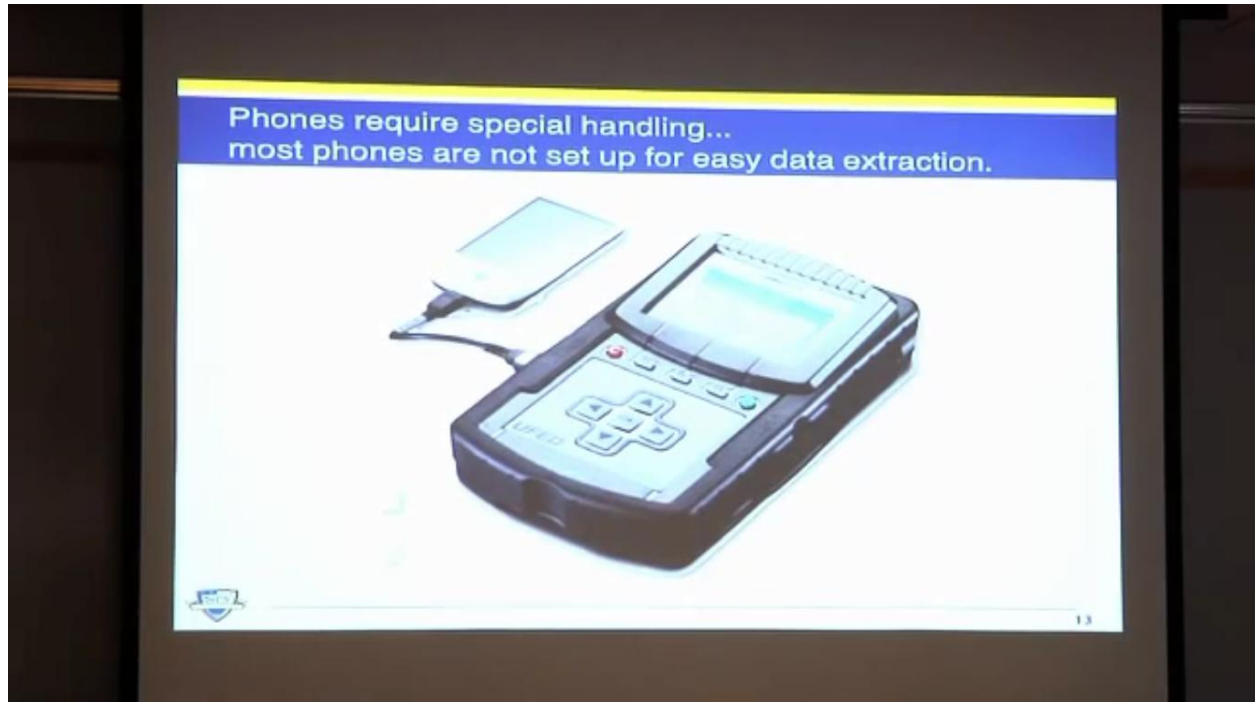


Original device stored in evidence locker.

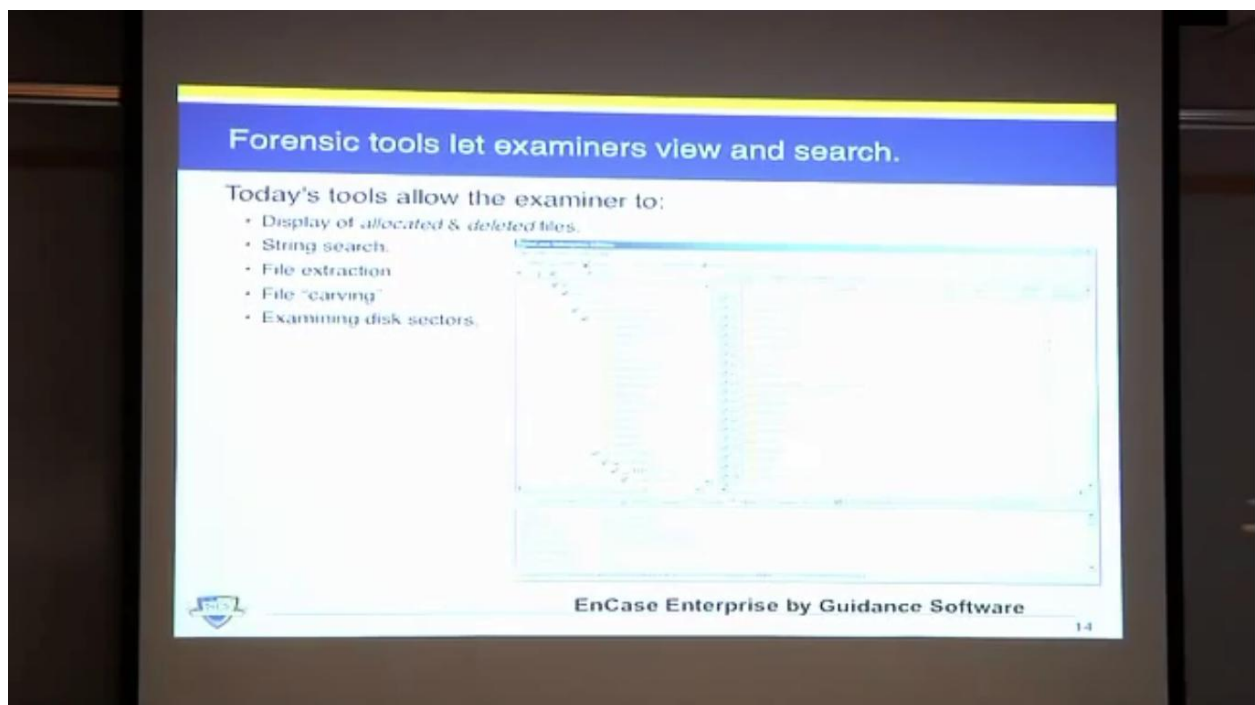
11

Tahap awal dari analisis yang dilakukan adalah ekstraksi data. Penggunaan disk untuk pengkopian dilakukan pada tahap ini, dan ini akan menjadi bahasan utama pada presentasi ini.

Untuk perangkat khusus seperti phone memiliki kebutuhan khusus untuk ekstraksi data yang ada didalamnya, dan aka nada kesulitan tersendiri.



Dalam pembacaan data forensic terdapat beberapa tahapan untuk menentukan hasil yaitu ada pada slide dibawah ini.




Beberapa ketentuan yang akan membebankan pembacaan dan pemrosesan data yaitu ada pada slide-slide berikut.

1 con't: Diversity is more than a multiplicity of file formats...

Data may be *inconsistent* or *incomplete*

- Files that are deleted or partially overwritten
- Incomplete database records
- Intentionally altered to avoid analysis



Data frequently have *no public specification*

- Hacker tools & malware
- Proprietary file formats

We need strategies for systematically addressing diversity

- Exploit similarity and correlation
 - Items of interest are frequently repeated
- Detect deliberate attempts to hide information
 - Eliminate the truth and the implausible, and whatever remains must be impossible (and therefore falsest)
 - "Impossible" data should be examined for steganography

47


2: Data scale — a never ending problem

Scale is continually identified as a DF problem

- *DFWS 2000*
- *"The major item affecting overall performance is data volume. The amount of data collected for analysis of this type is often quite large."*

Moore's law scales the targets

- We are using top-of-the-line system to analyze top-of-the-line systems
- We need to analyze in hours (or days) what a subject spent weeks, months or years assembling



∴ We will *never* outpace the performance curve.

Most "big data" solutions from other fields don't work well with DF

- They have bigger budgets per byte (CERN LHC: 1 \$/B/month)
- Data diversity — Physics data is less diverse than a hard drive data
- Our data fights back — CERN data is not compressed/encrypted/fragmented/malware
 - Data complexity dramatically increases I/O and compute requirements

48

3: Temporal diversity — a never-ending upgrade cycle

Today's DF tools must process:

- Today's computers / phones / cameras
 - *Because some criminals like to buy what's new!*
- Yesterday's computers / phones / cameras
 - *Because criminals are using old devices too!*



Implications for DF users and developers:

- Upgrade DF software as soon as possible.
- DF software will become geometrically more complicated over time....
 - ... or DF software will adapt on the fly to new data formats and representations.
 - *automated code analysis; pattern matching; hidden Markov models; etc.*



19

4: Human capital is bad all over — especially for DF

DF users (examiners, analysts):

- Overwhelmingly in law enforcement.
- Little or no background in CS or IS
- Deadline-driven; over-worked
- Knowledgeable users tend to focus in just one particular area.
 - *Result: It takes two years to train most DF examiners*



DF developers ("researchers"):

- Data diversity means developers need to know the whole stack
 - *opcodes & Unicode → OS & Apps → networking, encryption, etc.*
- Scale issues means developers need to know HPC:
 - *threading, systems engineering, supercomputing, etc.*
- Result:
 - *It's hard to find qualified developers*
 - *Developers must be generalists*



20

5: The "CSI Effect" — unrealistic expectations.

On TV:

- Forensics is swift.
- Forensics is certain.
- Human memory is reliable.
- Presentations are highly produced.



TV digital forensics:

- Every investigator is trained on every tool.
- Correlation is easy and instantaneous.
- There are no false positives.
- Overwritten data can be recovered.
- Encrypted data can usually be cracked.
- It is impossible to delete anything.



21

Ditemukan berbagai permasalahan dalam pemrosesan data forensic yang ditemukan secara nyata yaitu ada pada slide berikut.

The reality of digital forensics is less exciting.

There are lots of problems:

- Data that is overwritten cannot be recovered
- Encrypted data usually can't be decrypted
- Forensics rarely answers questions or establishes guilt or provides specific information
- Tools crash a lot
- DF tools look a lot like traditional tools



EnCase



Windows Explorer

Result:

- *DF is a difficult process that looks easy*
- *This is not a good place to be*



22

Sedangkan tool yang ada begitu mahal dan terbatas.

6: Digital Forensics tools — expensive with limited market

DF tools are expensive to develop:

- Data diversity
- Security critical
- High performance computing

Limited market:

- Consulting firms (more effective tools *decreases* billable hours)
- Police departments (not known for \$\$)
- Defense (not known for major DF expenditures)

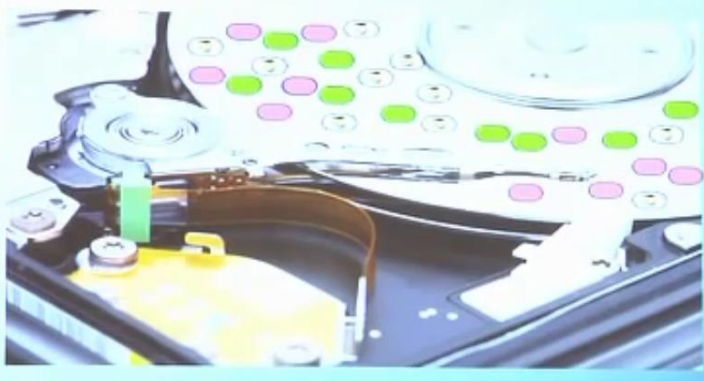
My personal experience:

- It's very hard to stay in business as a tool developer
- Government should have an ongoing role in funding DF research and tool development
- Open source software frequently makes the most sense
 - *Open Source preserves investment, enables future research, empowers users.*




23

Terobosan yang diberikan oleh pembicara yaitu kecepatan analisis dengan menggunakan random sampling



High Speed Forensic Analysis
with Random Sampling



Can we analyze a 1TB hard drive in five minutes?

US agents encounter hard drives at border crossings...



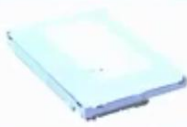

Searches turn up rooms filled with servers....



26

Pemborosan waktu dari kalkulasi yang didapatkan dengan membaca 1TB hard drive yaitu sebagai berikut.

If it takes 3.5 hours to read a 1TB hard drive, what can you learn in 5 minutes?

		
Minutes	208	5
Max Data	1 TB	36 GB
Max Seeks		90,000

36 GB is a lot of data!

- Only $\approx 2.4\%$ of the disk...
- But it can be a *statistically significant sample*



27

Alokasi data yang akan digunakan untuk analisis adalah sebanyak berikut ini.

Resident data is the data you see from the root directory.
"Allocated" files.

```
graph TD; Root[" / "] --> tmp[" tmp "]; Root --> usr[" usr "]; Root --> bin[" bin "]; tmp --> a[" a "]; tmp --> b[" b "]; usr --> slg[" slg "]; bin --> ls[" ls "]; bin --> cp[" cp "]; bin --> mv[" mv "]; slg --> beth[" beth "]; slg --> mail[" mail "]; slg --> junk[" junk "];
```

Resident Data

31

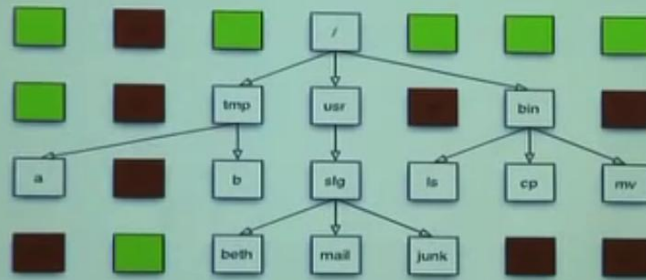
"Deleted data" is on the disk,
but can only be recovered with forensic tools.

```
graph TD; Root[" / "]; Root --> tmp[" tmp "]; Root --> usr[" usr "]; Root --> bin[" bin "]; tmp --> a[" a "]; tmp --> b[" b "]; usr --> slg[" slg "]; bin --> ls[" ls "]; bin --> cp[" cp "]; bin --> mv[" mv "]; slg --> beth[" beth "]; slg --> mail[" mail "]; slg --> junk[" junk "];
```

Deleted Data

32

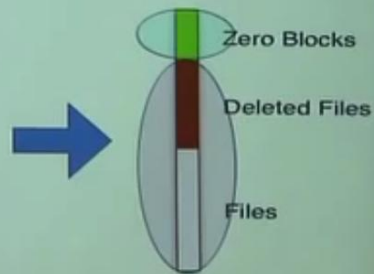
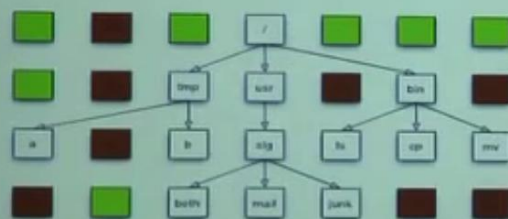
Some sectors are blank.
They have "No data."



No Data

33

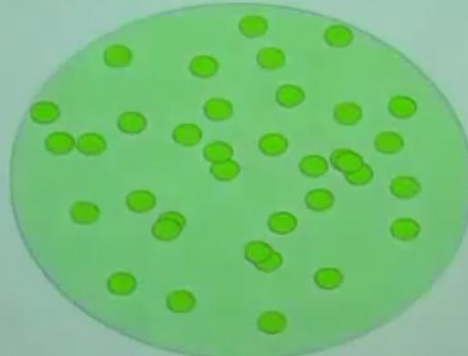
Sampling can't distinguish *allocated* from *deleted* data.



34

Dengan beberapa sector yang terbagi atas zero block, deleted files dan file akan membebani tahapan analisis dari data forensic.

A 1TB drive has 2 billion sectors.
What if we read 10,000 and they are all blank?



Chances are good that they are all blank.



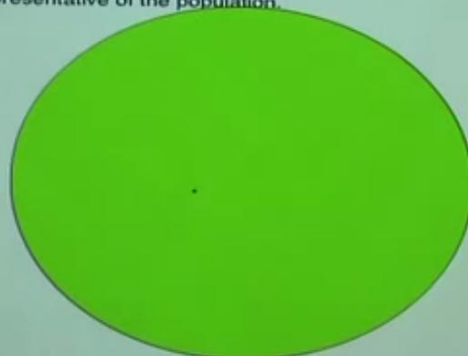
37

Dengan data yang diasumsikan seperti slide diatas adalah pemborosan waktu hanya untuk sector blank.

Random sampling *won't* find a single written sector.

If the disk has 1,999,999,999 blank sectors (1 with data)

- The sample is representative of the population.



We will only find that 1 sector with exhaustive search.



38

Oleh karena itu penggunaan sampling untuk analisis akan sangat memberikan perubahan yang nyata.