Keamanan Jaringan Komputer
Digital Forensic

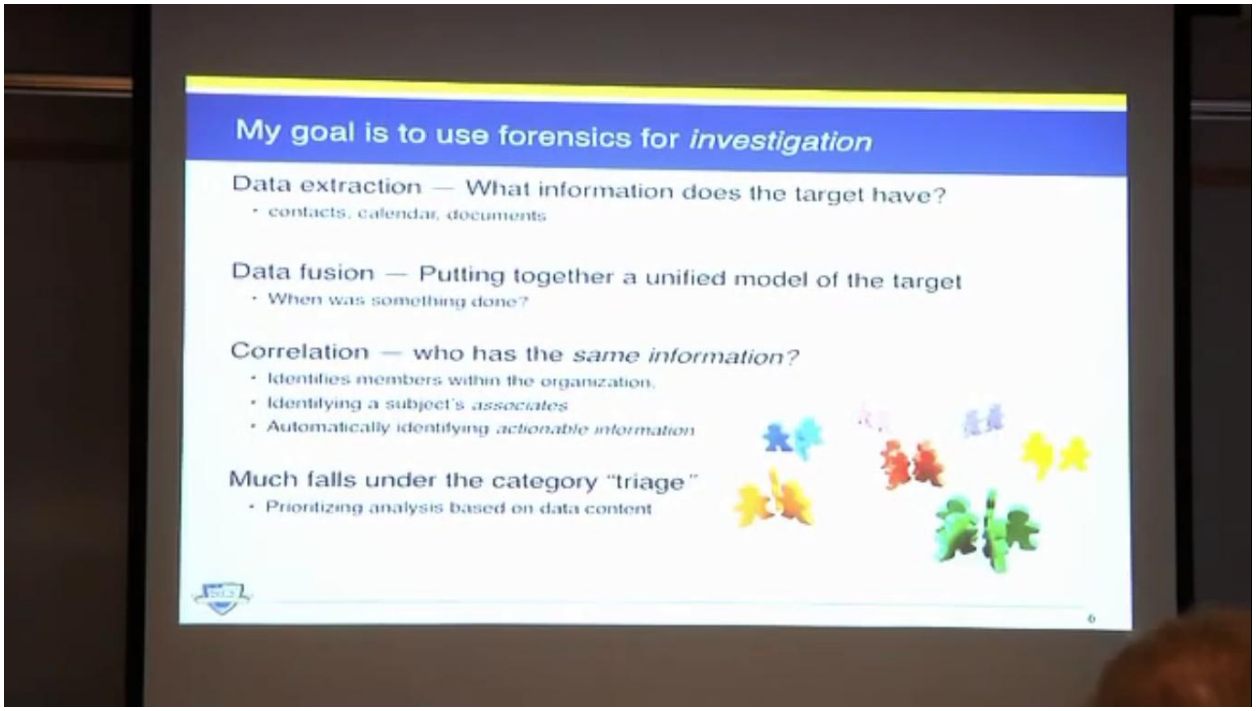
Disusun Oleh :
Nama : Imam Mustofa
NIM : 09011181320028

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017

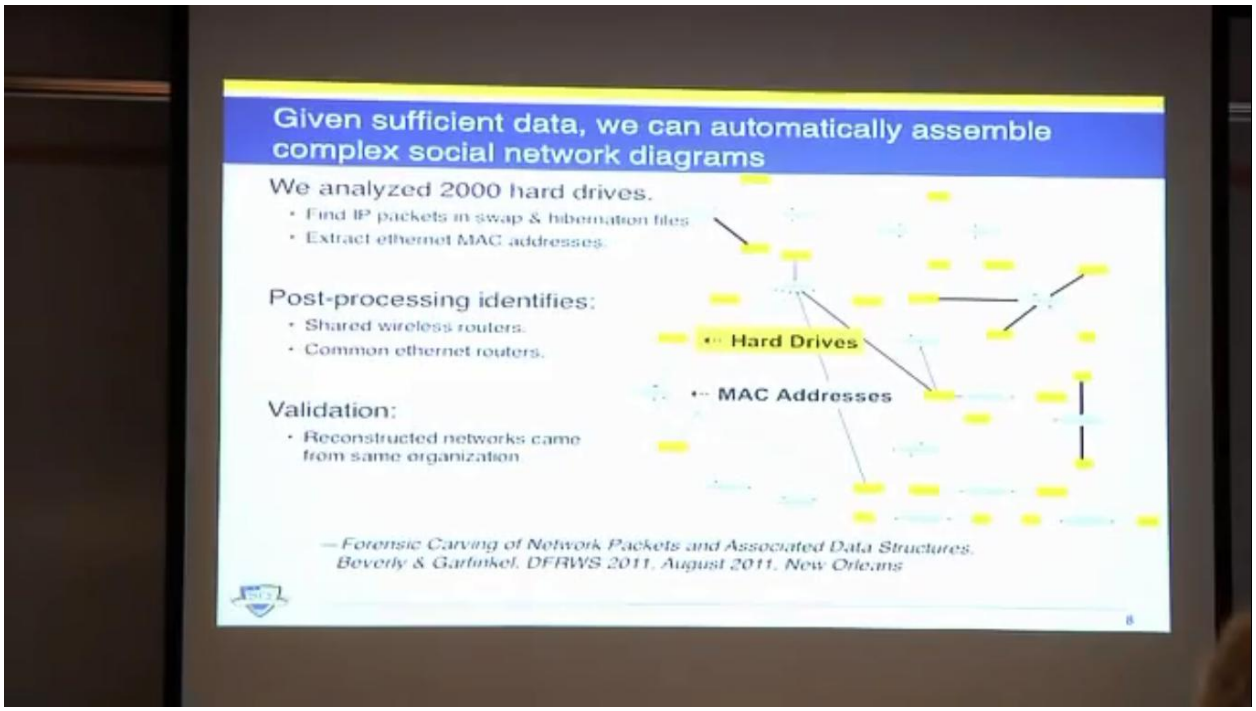
Informasi yang dibawakan oleh pembicara dibawah ini adalah sebuah terobosan inovasi dalam pengambilan data dengan kecepatan tinggi terhadap data-data forensic.

Pada tampilan slide diatas yang merupakan perjalanan identitas dari pembicara.

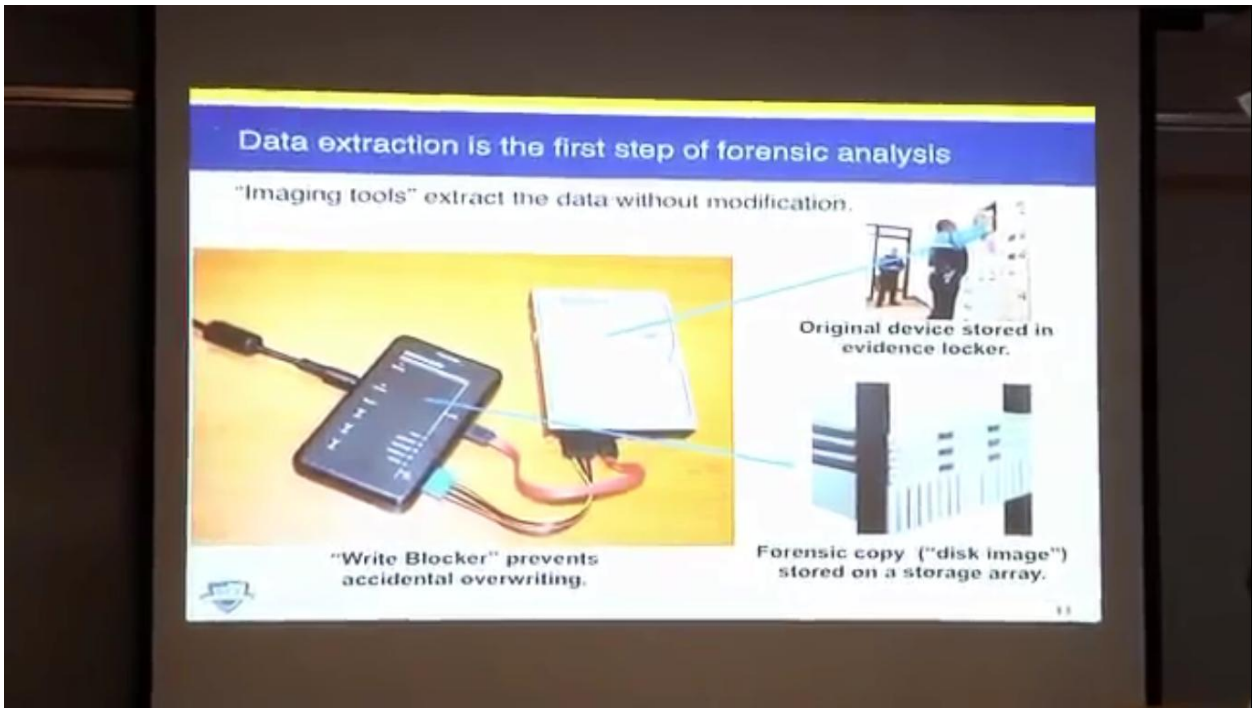
Yang dijelaskan pertama kali dalam presentasi yang dilakukan adalah mengenai digital forensic mulai dari caranya yang tradisional kepada sesuatu hal



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

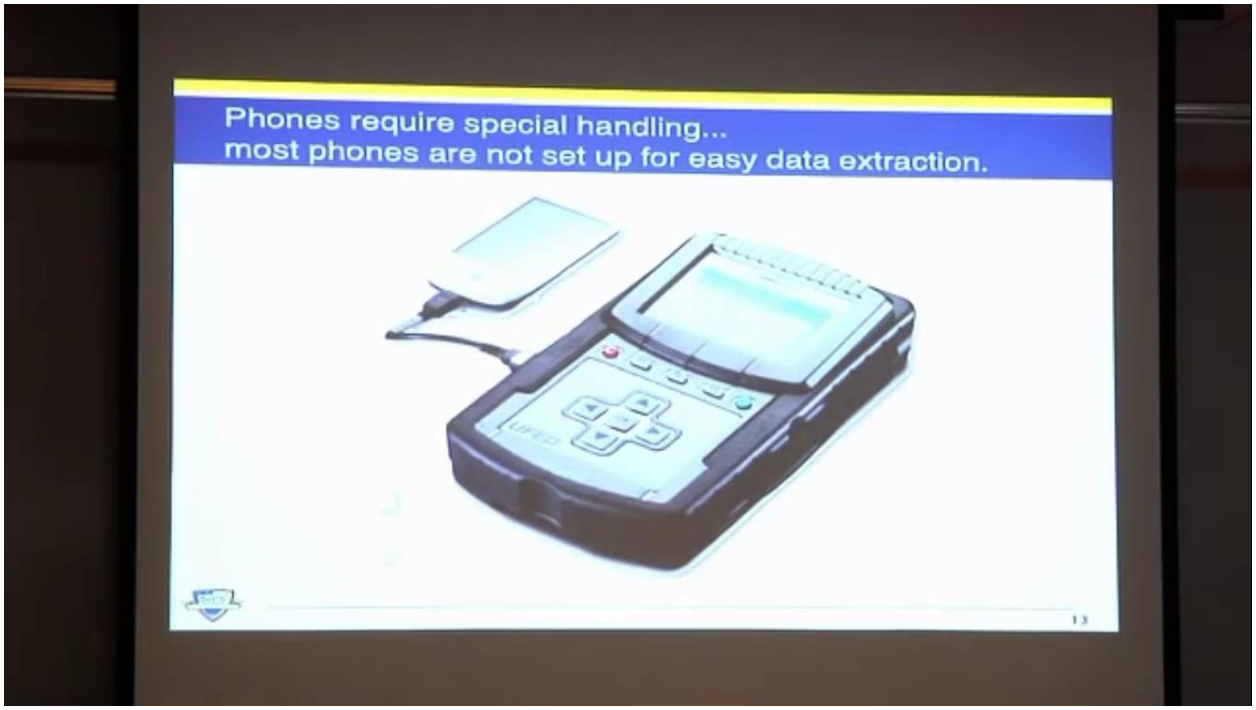


Pembicara menerangkan proses pengolahan data dengan jumlah dan criteria yang diinginkan sehingga membentuk diagram tersendiri, yang ditekankan pada slide diatas bahwa setiap pengiriman data akan mendapatkan mac address dari dua hal yaitu komputer sumber dan dari router.

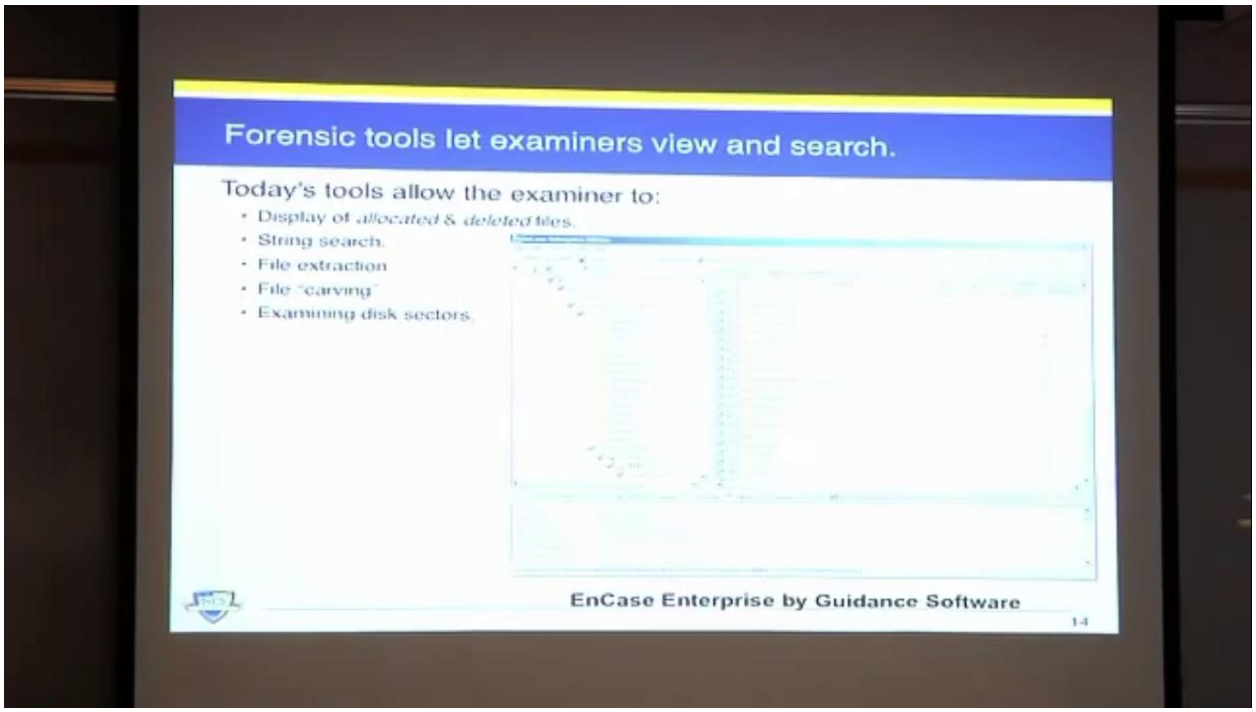


Tahap awal dari analisis yang dilakukan adalah ekstraksi data. Penggunaan disk untuk pengkopian dilakukan pada tahap ini, dan ini akan menjadi bahasan utama pada presentasi ini.

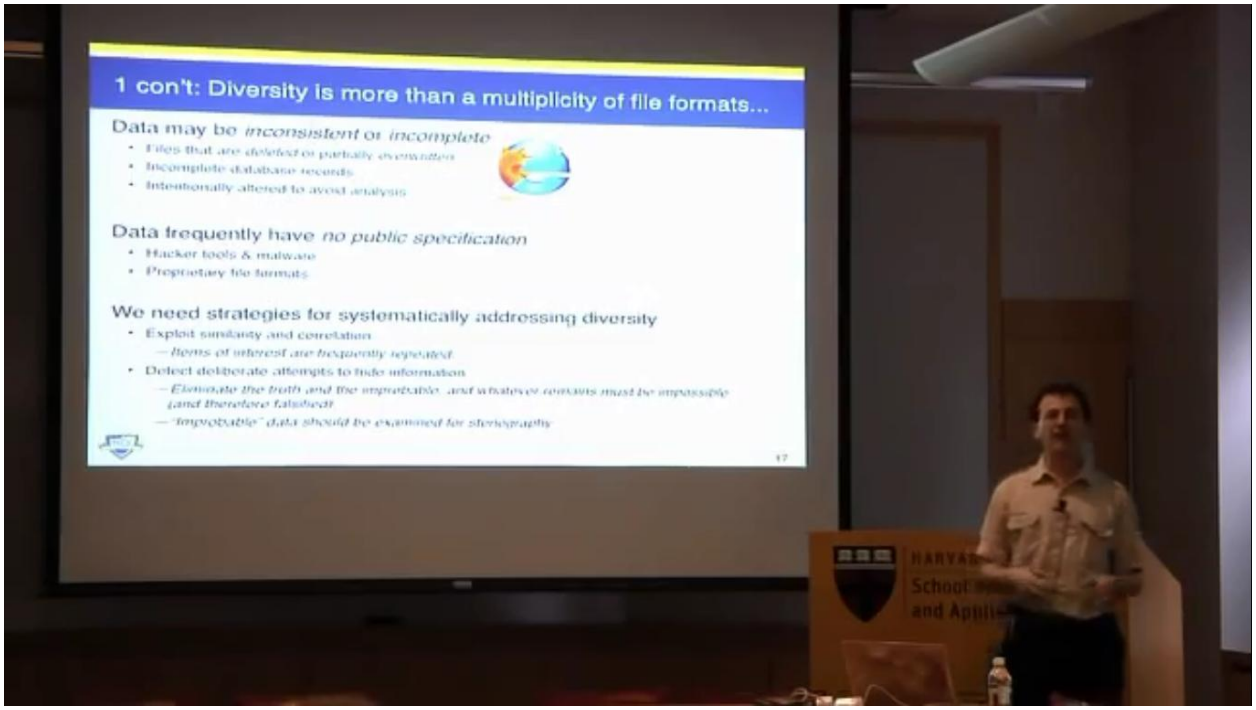
Untuk perangkat khusus seperti phone memiliki kebutuhan khusus untuk ekstraksi data yang ada didalamnya, dan aka nada kesulitan tersendiri.

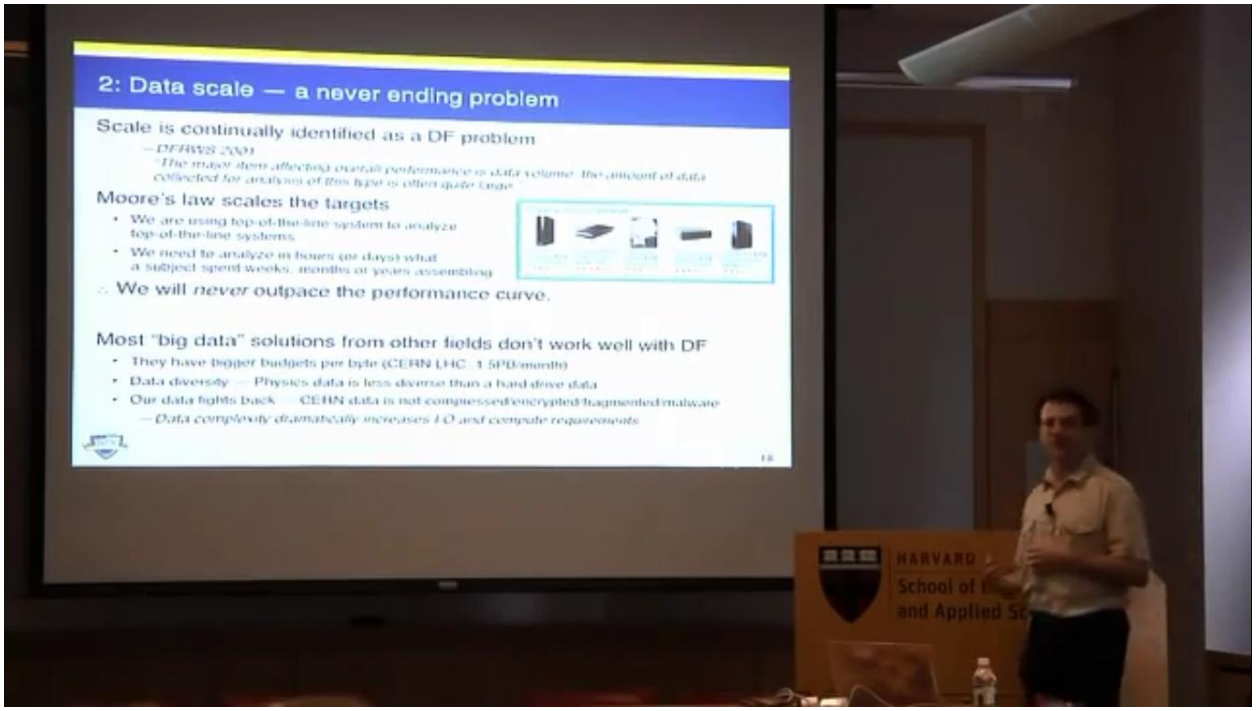


Dalam pembacaan data forensic terdapat beberapa tahapan untuk menentukan hasil yaitu ada pada slide dibawah ini.



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





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.*

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
- Knowledgable 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*

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 pda 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

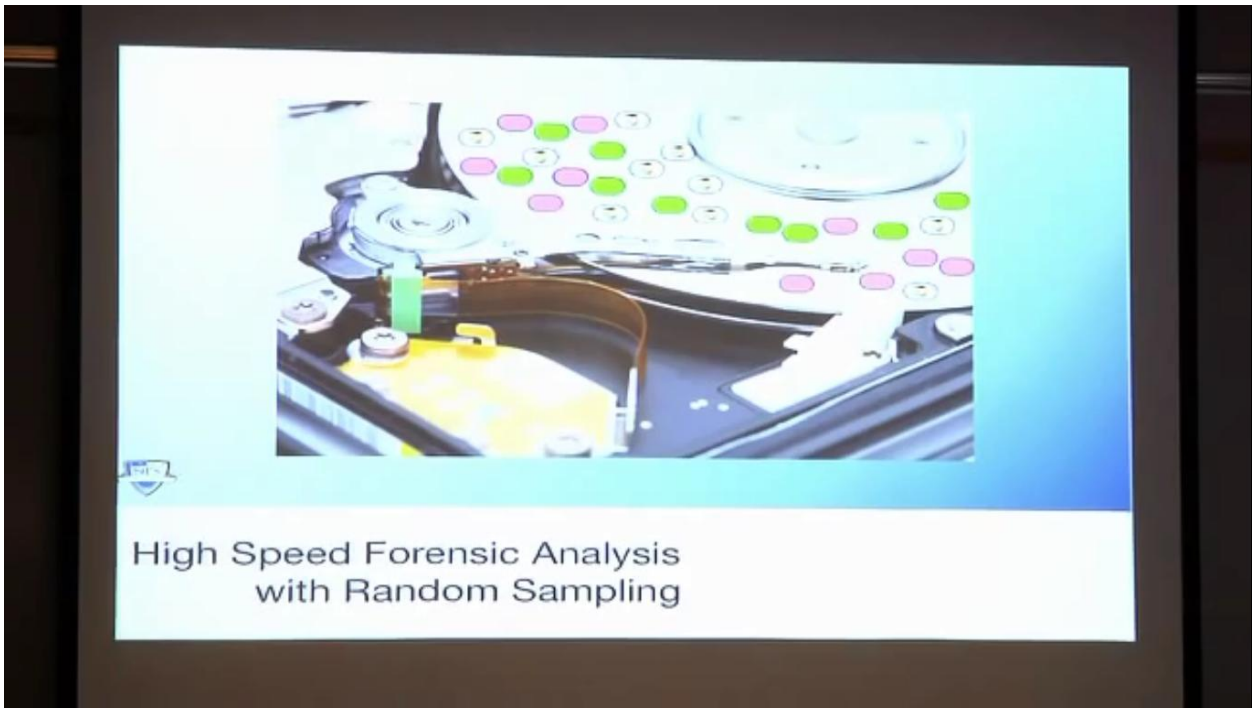
Result:

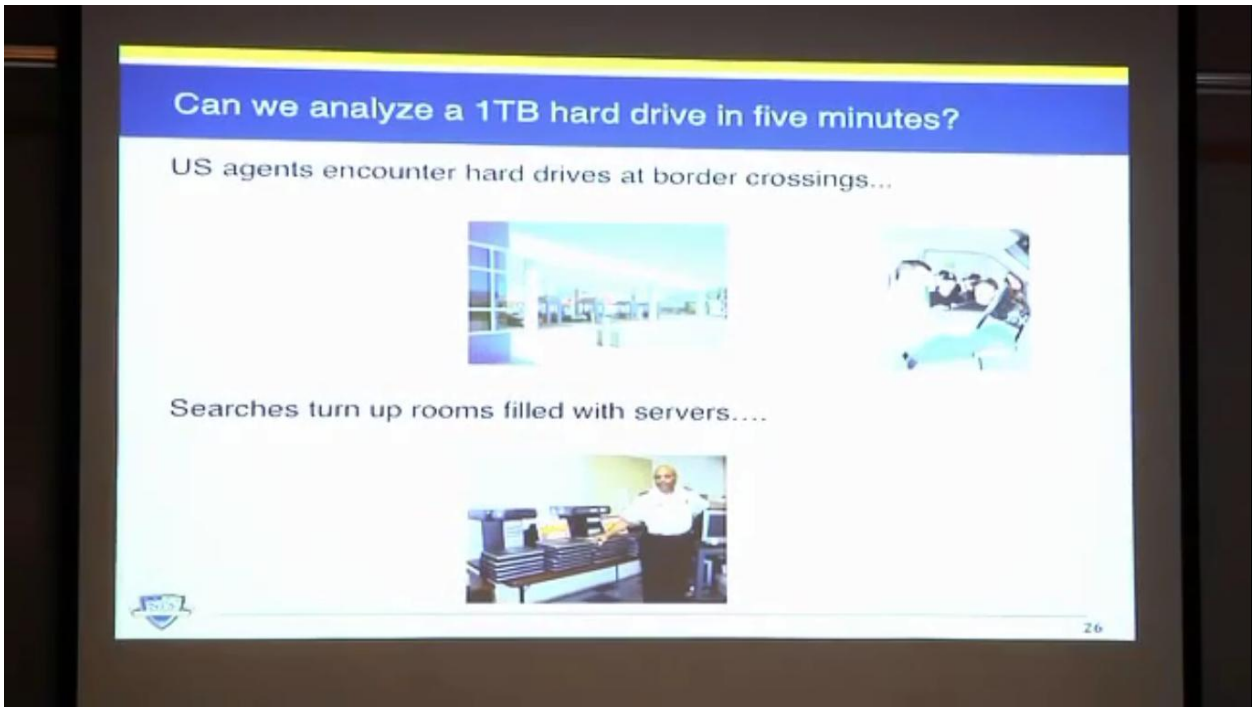
- *DF is a difficult process that looks easy*
- *This is not a good place to be*

22

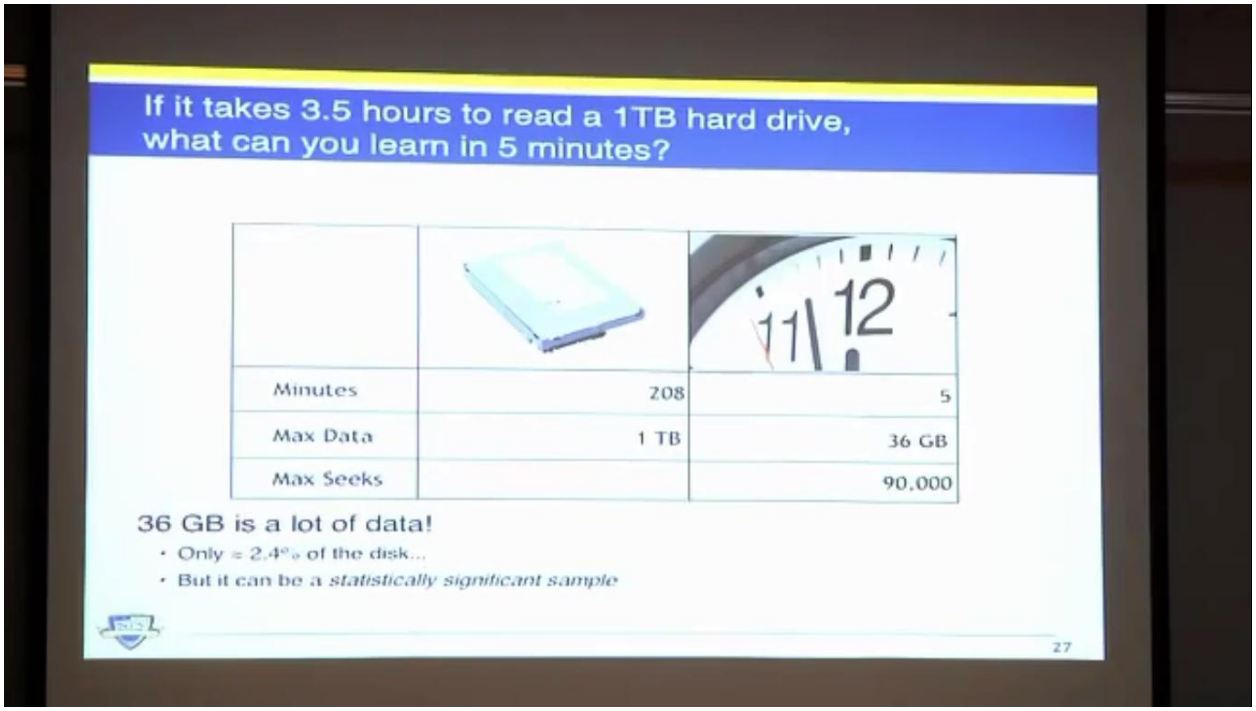
Sedangkan tool yang ada begitu mahal dan terbatas.

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

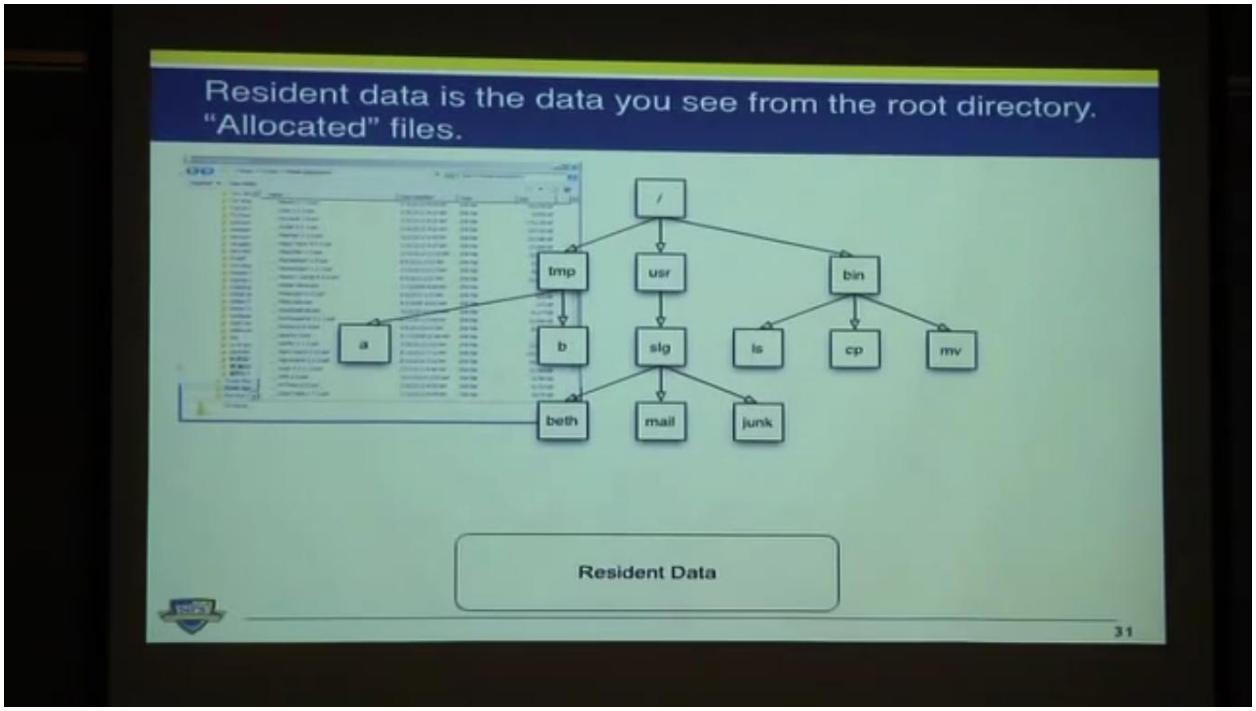


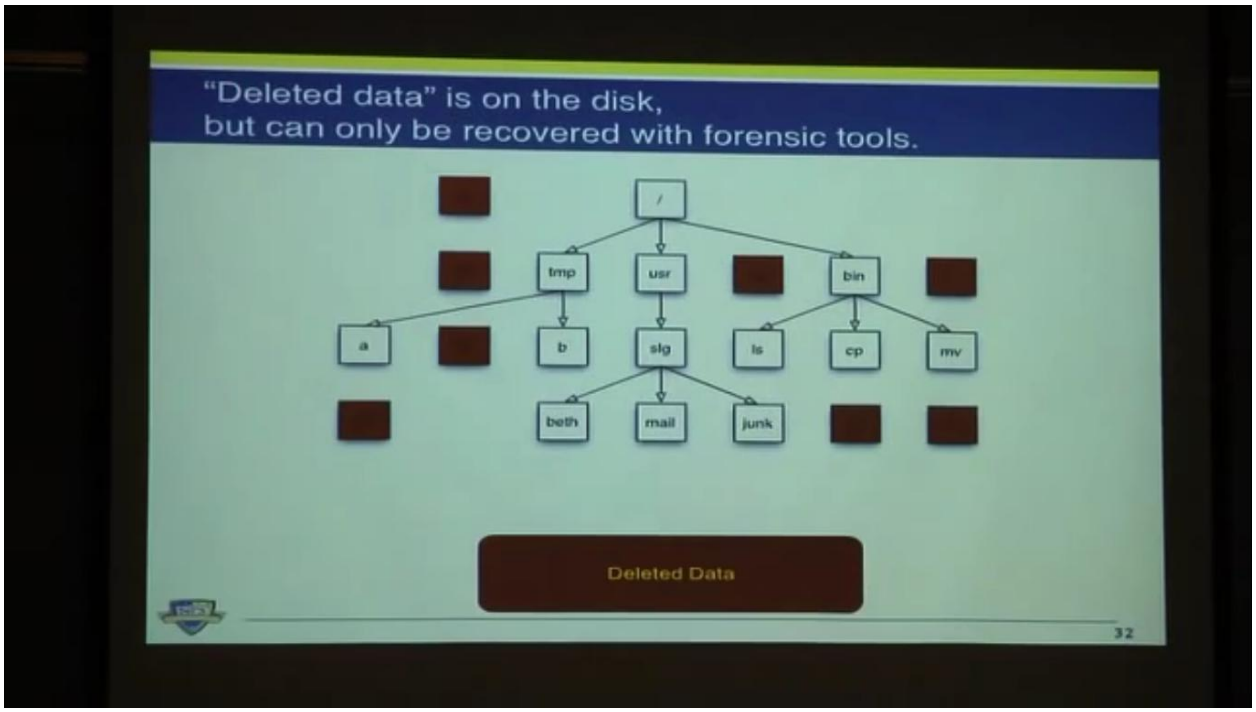


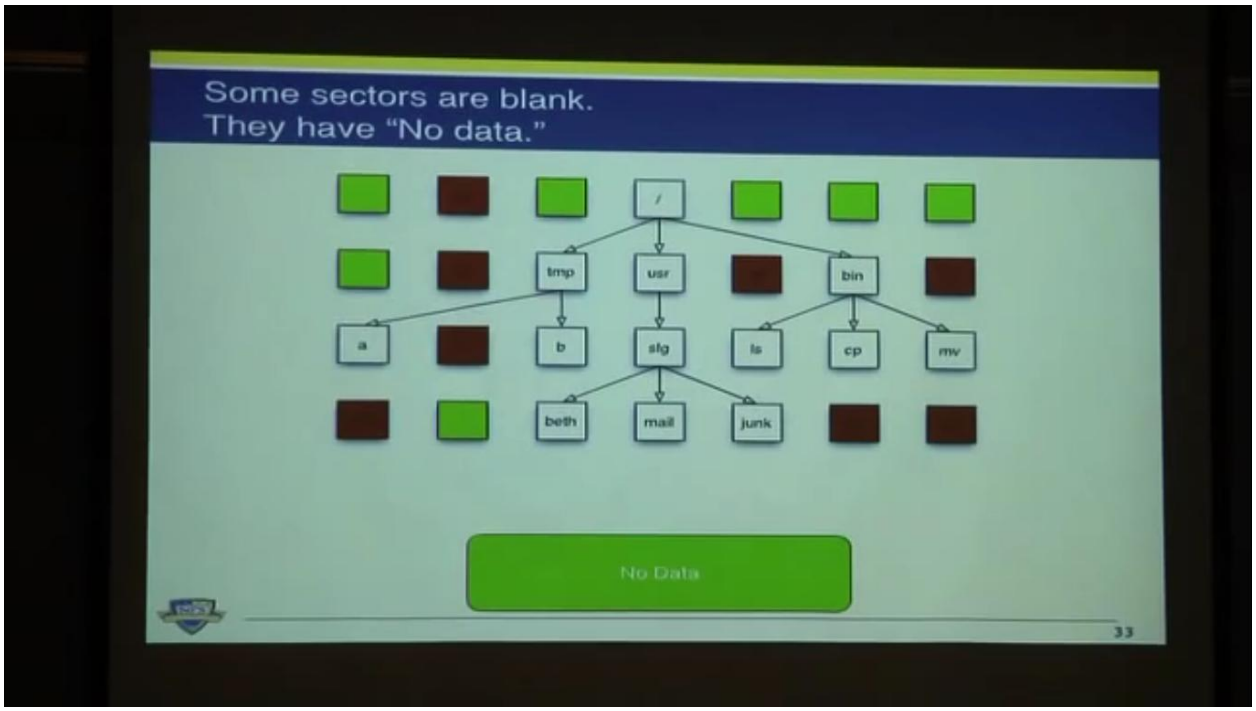
Pemborosan waktu dari kalkulasi yang didapatkan dengan membaca 1TB hard drive yaitu sebagai berikut.

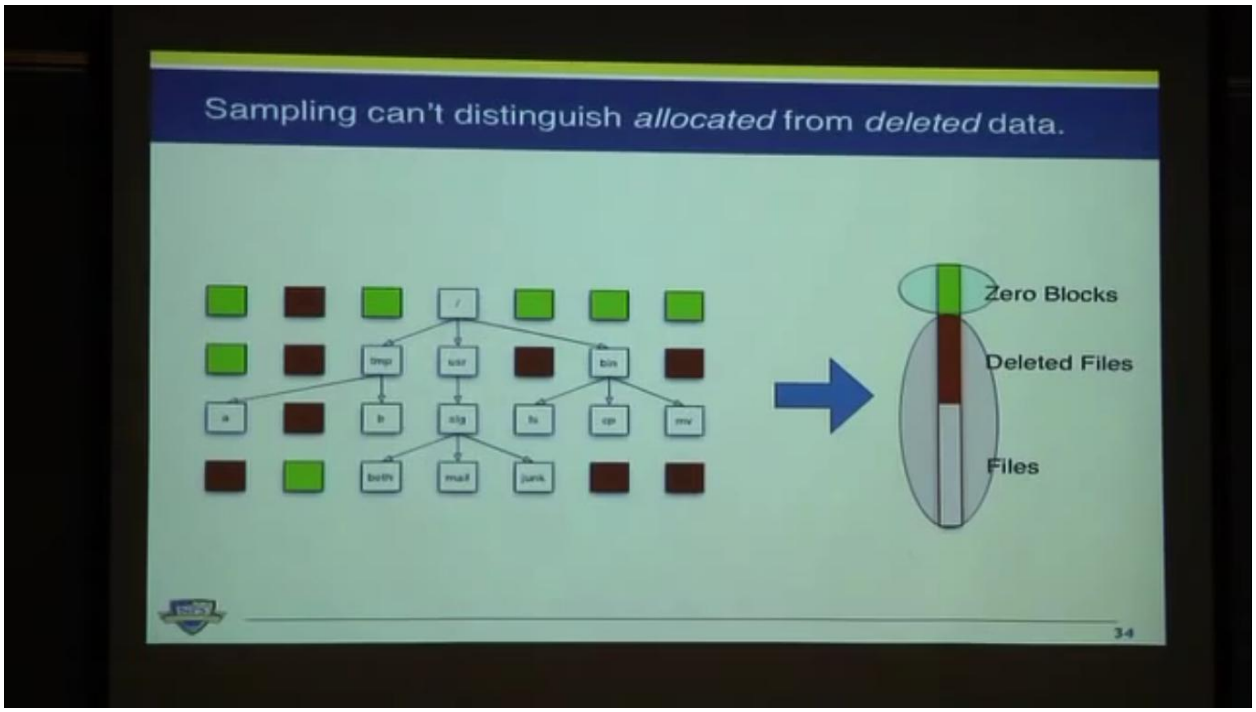


Alokasi data yang akan digunakan untuk analisis adalah sebanyak berikut ini.

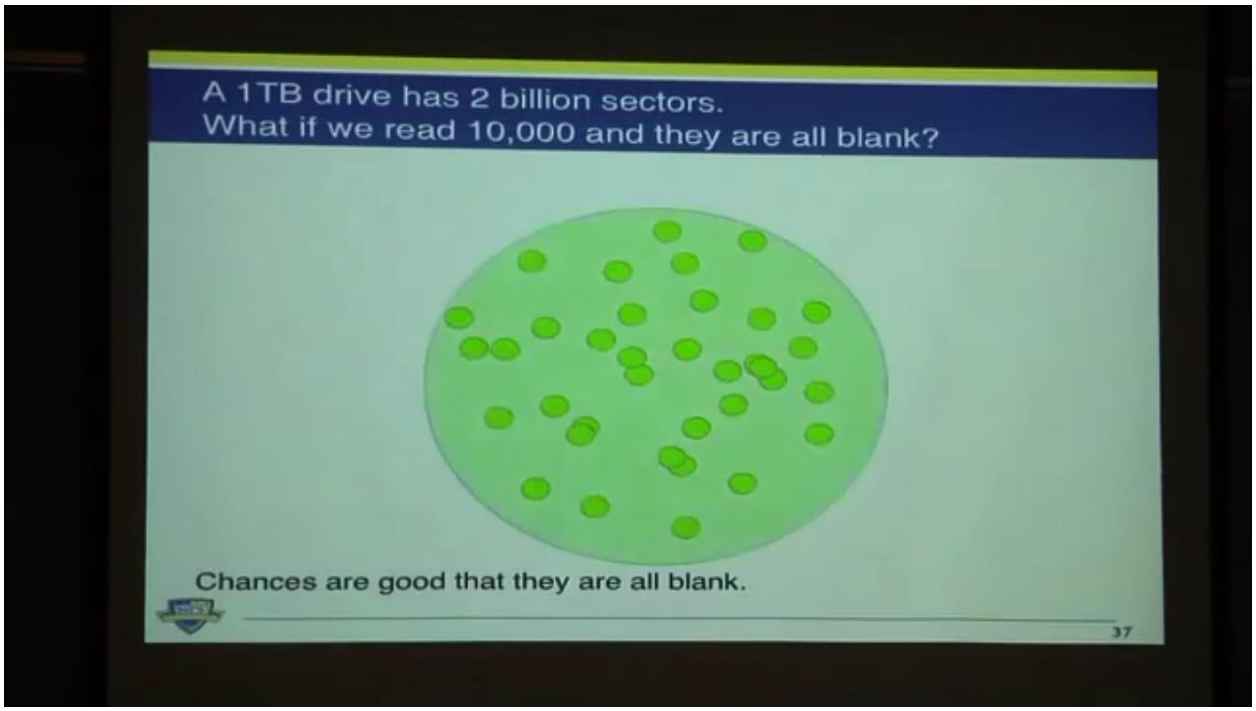




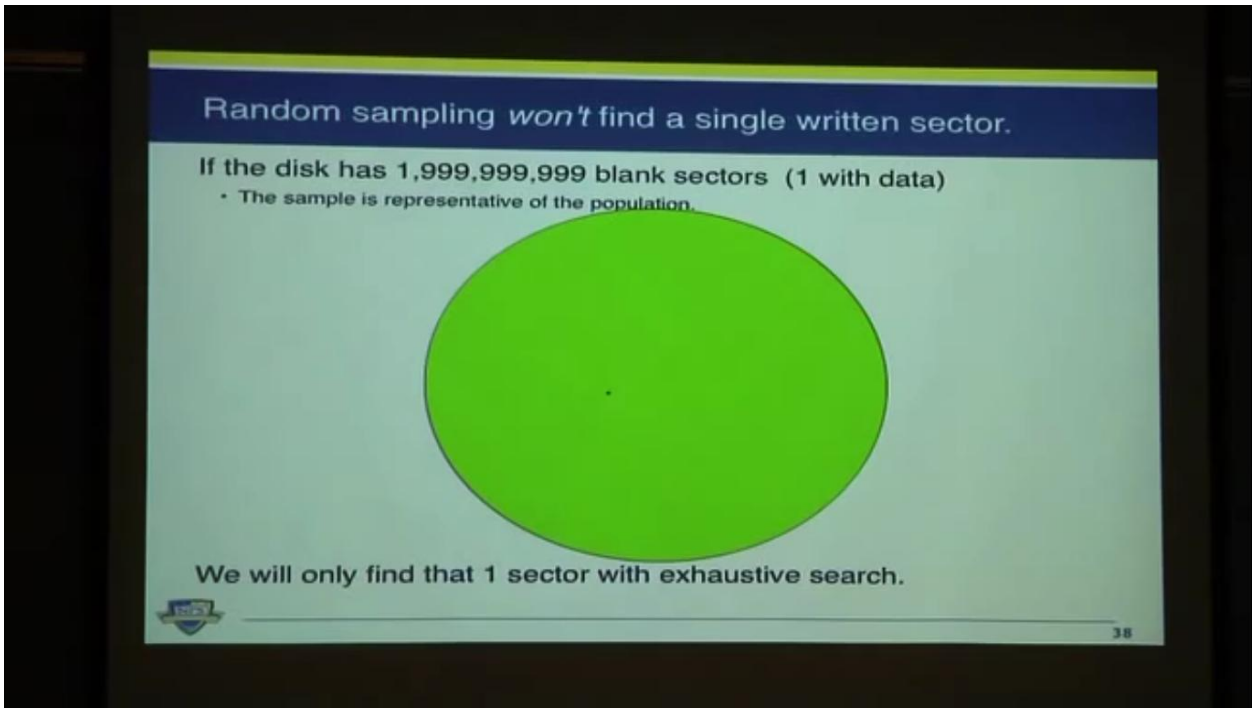




Dengan beberapa sector yang terbagi atas zero block, deleted files dan file akan membebani tahapan analisis dari data forensic.



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



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