University of South Wales
Prifysgol De Cymru

Information Assurance in a Distributed Forensic Cluster

Nick Pringle[a]*, Mikhaila Burgess[a]

[a] *University of South Wales (formerly University of Glamorgan), Treforest, CF37 1DL, UK*

INFORMATIONSECURITY RESEARCHGROUP

© University of South Wales

Introduction

- As data quantities increase we will need to adopt alternative models in our forensic processing environments.
- We believe that Distributed Processing will play a key part in this.
- We believe existing practice breaks down in a distributed system.
- We're going to show our design for a framework that provides data assurance in a distributed storage environment.

© University of South Wales

“Forensic Soundness”

- It’s a key part of our discipline
- It’s quite hard to define
- Existing standards and frameworks are a little vague
- It’s all down to accepted Best Practice
- It’s achieved by implementing ‘controls’

© University of South Wales

‘Internal Controls’ on the Forensic Process

- By **Property**, eg. cryptographic hashes, sizes, name!
- By **Location**, eg. on specific media, network storage
- By **Authority**, eg. order and response form
- By **Access Control**, eg. write blocker, password
- By **Separation** of Process, eg. crime scene and lab work
- By **Checklist**, eg. have all the tasks been completed?
- By **Audit**, but this is after the process

© University of South Wales

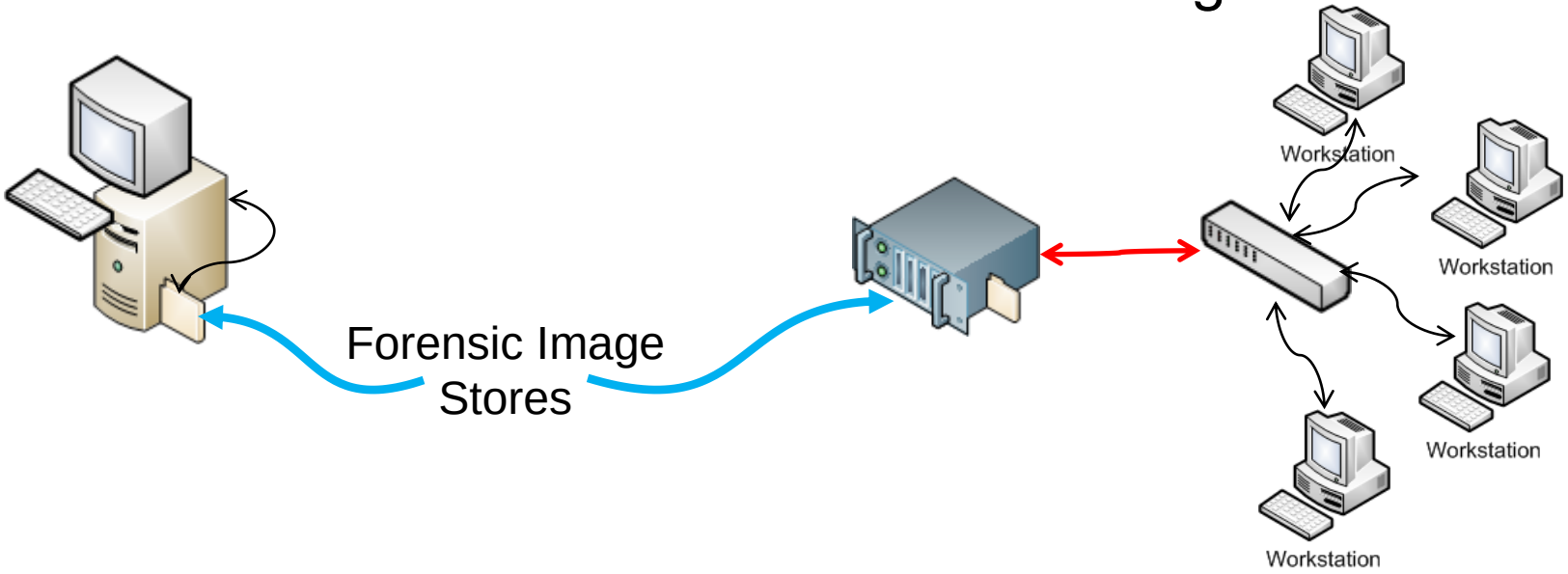
At the bedrock of Forensics

- **The Forensic Image**
  - It's a snapshot at a point in time
  - It is complete,
    including Boot Sectors, Unallocated space, HPA, HPC areas
  - Rather like the pieces of a Jigsaw, the parts form a whole.
  - We can measure it with SHA-1 etc

© University of South Wales

‘Traditional’ Architectures

Based around a ‘Forensic Image’



© University of South Wales

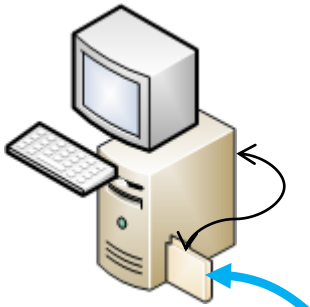
A time of Great Change

- In ‘the Golden Age’ life was so simple (Simson Garfinkel, 2010)
- 3V – Volume, Variety and Velocity (Gartner, 2007)
- We now have Desktops, notebooks, netbooks, Virtualisation, Cloud storage, Cloud Processing, Smart Phones, Tablets, SatNav, USB Sticks, Memory cards, Terabyte drives, games machines, Cameras, etc.
- We find it difficult to cope with the sheer volume of data
- We have a backlog

© University of South Wales

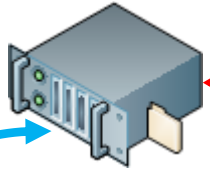
‘Traditional’ Architectures

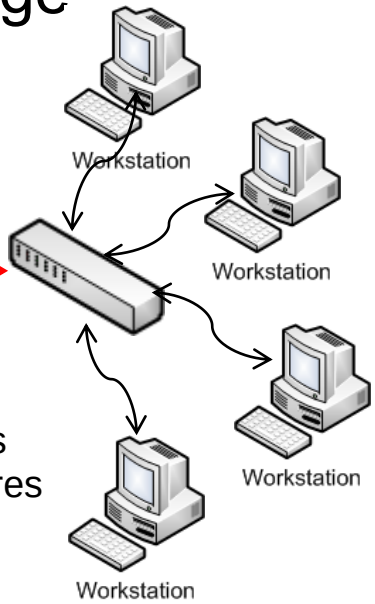
Based around a ‘Forensic Image’



This is limited to
SATA3 and 32 cores?

Forensic Image
Stores





SATA3 = 600MB/s
SSD Read = 500MB/s
If 1 Core can process 4 MB/s
This could occupy 150 cores
Processor constrained

Gigabit Network = 100MB/s
This can supply only 50 cores
Network constrained

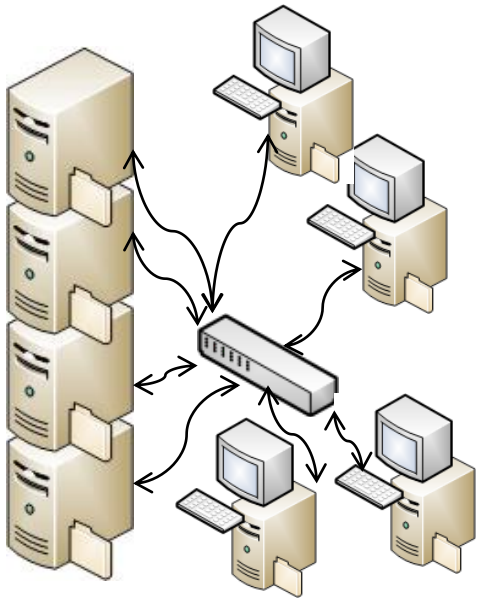
© University of South Wales

Anticipated Developments

- Multi tera-byte crime scenes
- Multi-Agency Access
- Multi Device Analysis
- Complex processing,
  - image and object recognition
  - Semantic meaning of text
  - usage profiling
- Google had the same type of Problem

© University of South Wales

Google/Apache Hadoop



A processing Model - Map/Reduce
A File System - HDfs

1. Split the data as whole files (SIPs/DEBs) across the cluster

   and

2. Don't move the data
   Run the program
   where the data is stored

© University of South Wales

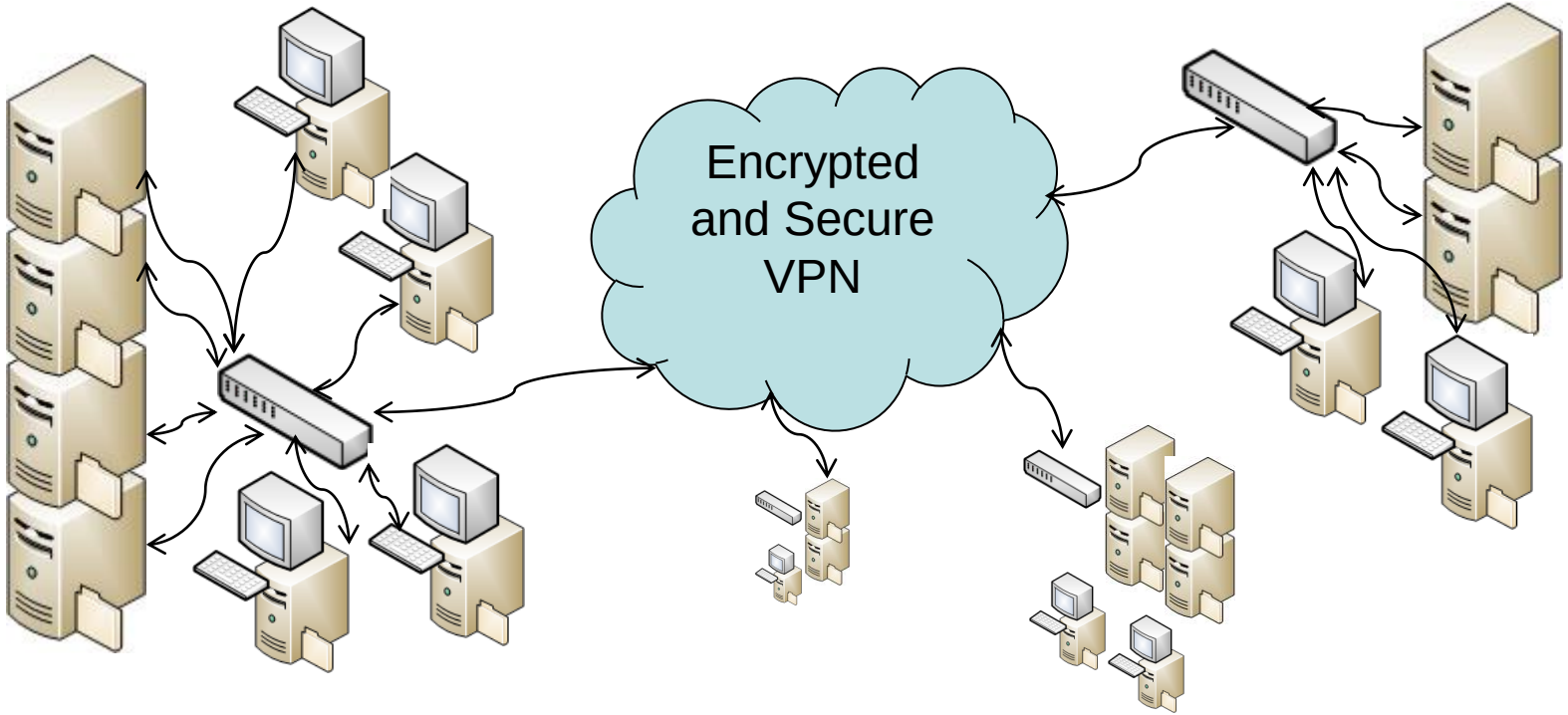
Solutions and Opportunities

Distributed processing is one that interests me

Application Layer	New Analysis Techniques Greater Volumes of data Require more processing power	Analyse and Visualise email from Enron PSTs
Middleware	A complete solution that allows distributed processing while satisfying the requirements of the legal profession of chain of evidence and validation	Acquisition Distribution Storage Processing Redundancy Job Management
OS Layer		Mix of Linux and Windows

© University of South Wales

Distributed Architecture



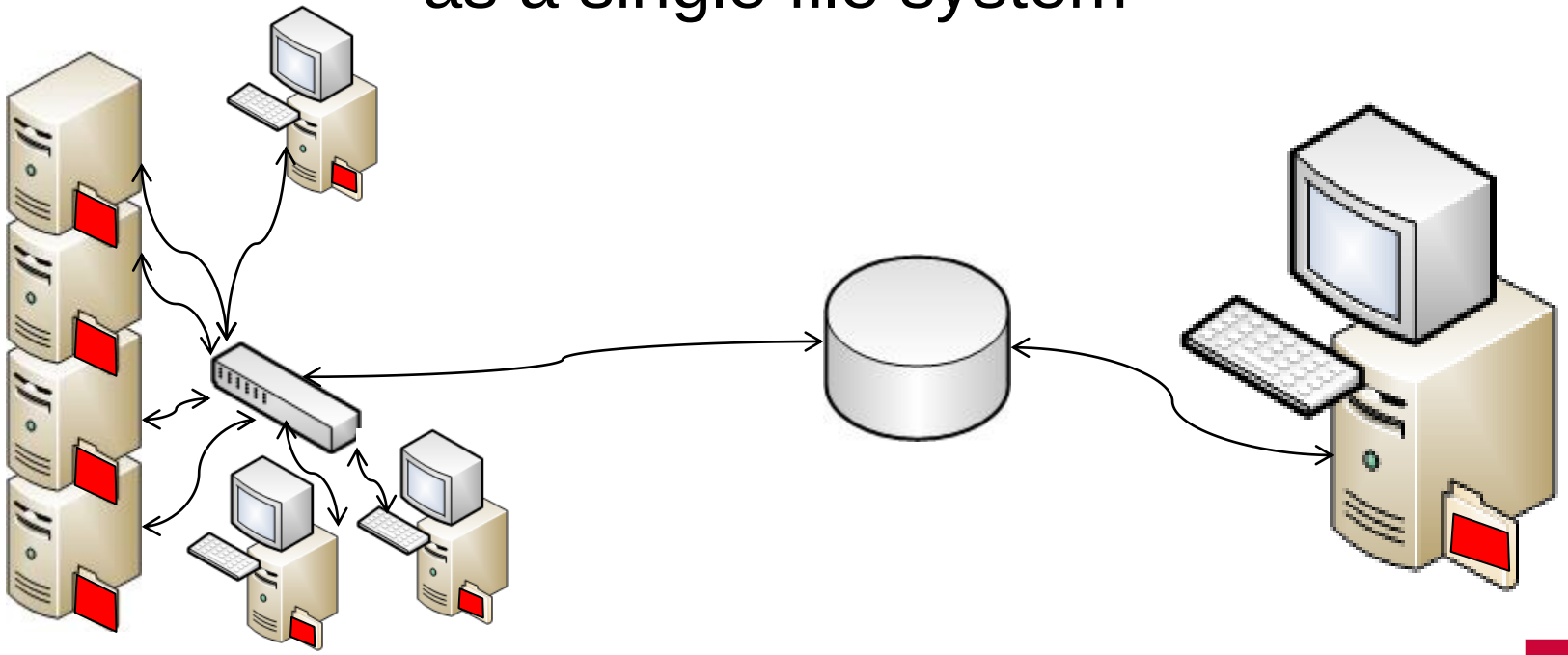
© University of South Wales

We lose “The Image”

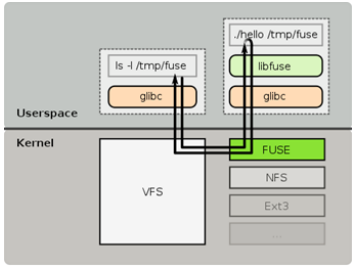
- Distributed storage of acquired information packages is in direct conflict with ‘the image’
- The image’s integrity comes, primarily, from it’s wholesomeness
- We lose the integrity we have enjoyed for 20 years
- We need to re-establish Assurance

© University of South Wales

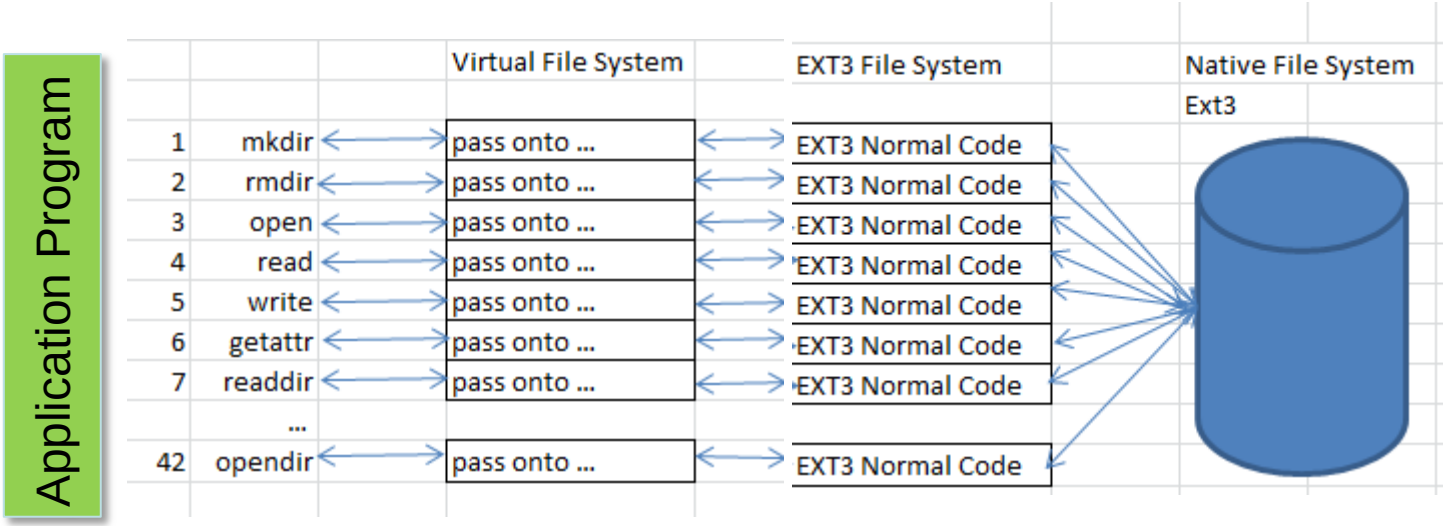
Distributed Data needs to appear as a single file system



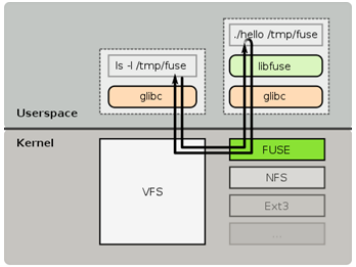
© University of South Wales



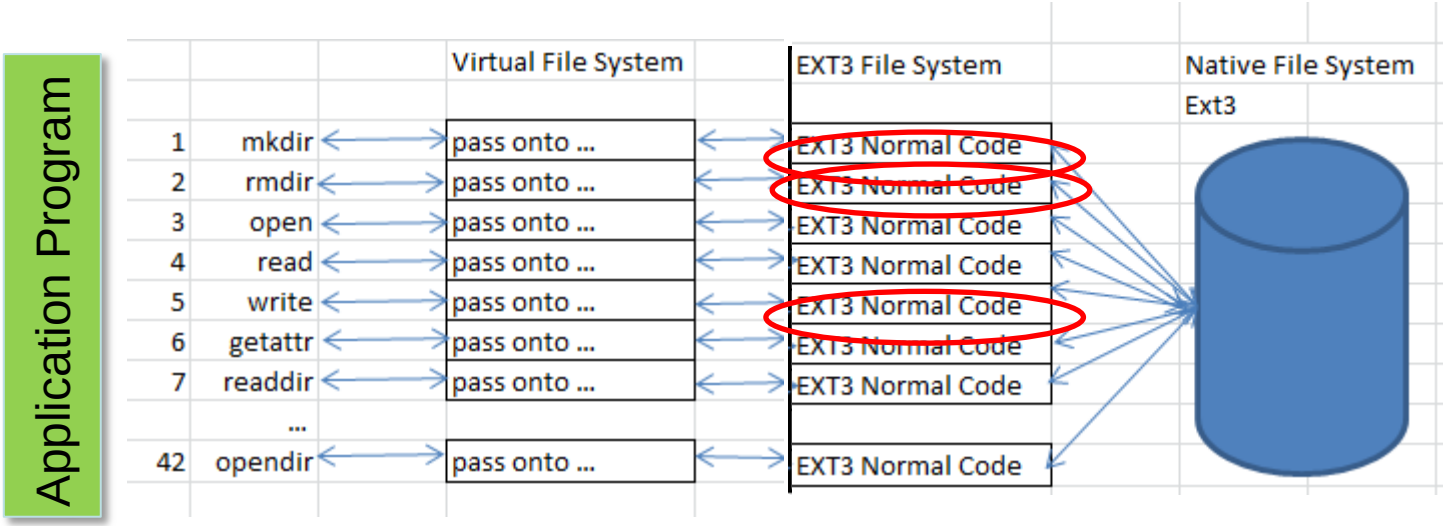
FUSE File-Systems



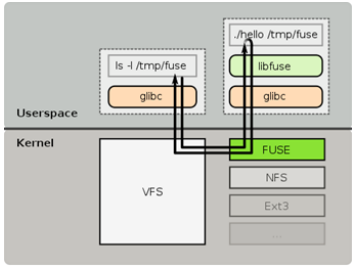
INFORMATIONSECURITY RESEARCHGROUP
© University of South Wales
University of South Wales
Prifysgol De Cymru



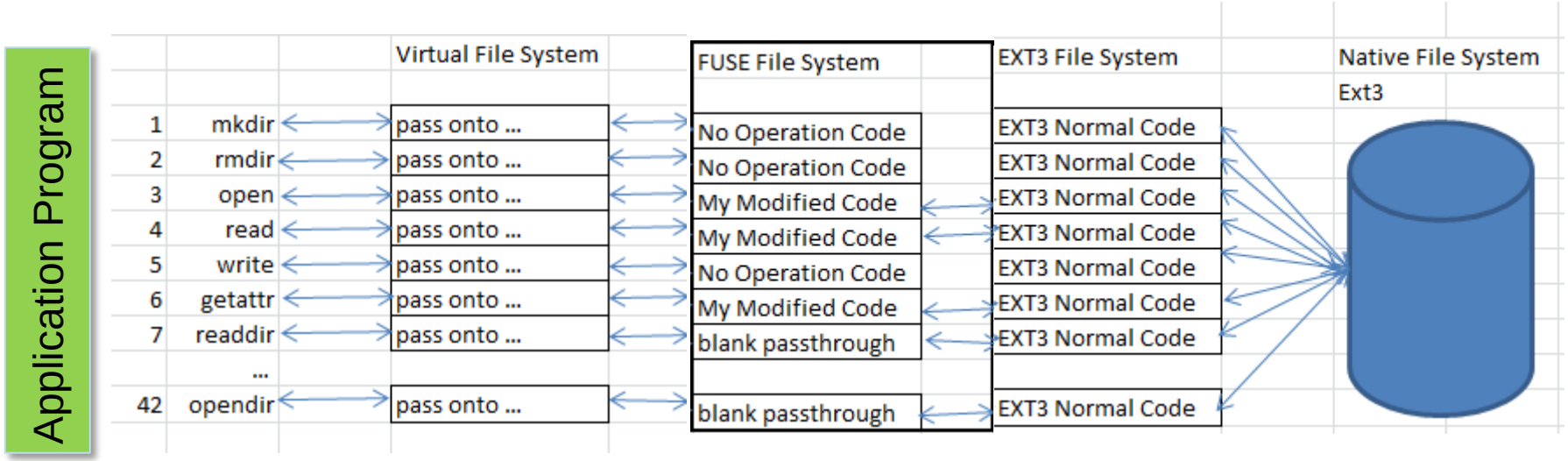
FUSE File-Systems



INFORMATIONSECURITY RESEARCHGROUP
© University of South Wales
University of South Wales
Prifysgol De Cymru



FUSE File-Systems



© University of South Wales

FUSE File System in Forensics

- Forensic discovery auditing of digital evidence containers, Richard, Roussev & Marziale (2007)
- Selective and intelligent imaging using digital evidence bags. In: Proceedings of the sixth annual digital forensics research workshop (DFRWS), Lafayette, IN; Aug 2006. Turner P.
- Affuse (Simson Garfinkel)
- MountEWF
- Xmount for VirtualBox or VMWare format disk images.

© University of South Wales

FClusterfs – A wish list

- The ability to store extended directory/file meta data
- We want unaltered legacy software to run. New software requires no new skillset. Sculptor, bulk_extractor etc will still work
- Gives access to files on remote servers where they're stored as whole files
- The ability to handle multi storage volumes from different media
- Has end to end encryption built-in
- Tracks movements and processing: Logging.
- Is Read Only to the user
- Highly tailorable access control at volume, directory and file levels

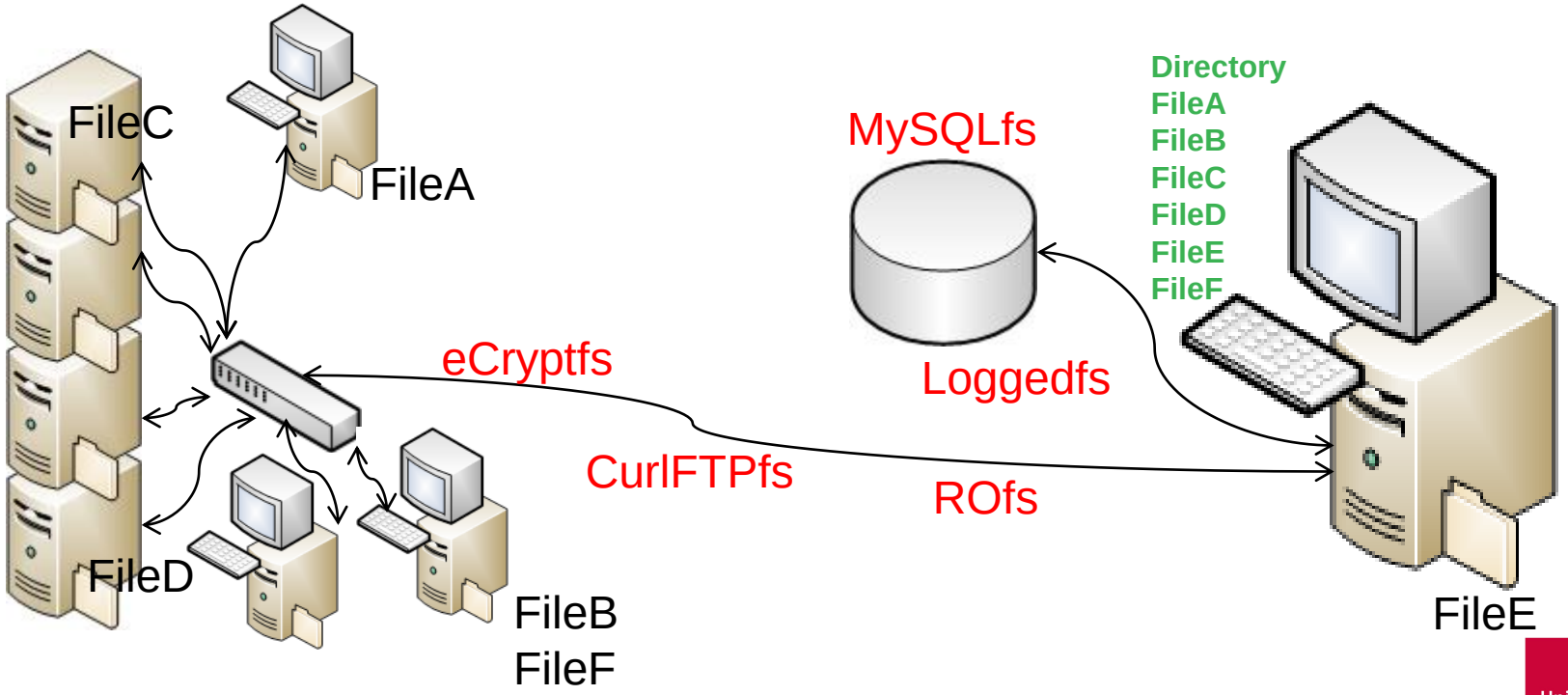
© University of South Wales

Existing FUSE File-Systems

- MySQLfs - Substitutes an SQL database for the file-system
- CurlFTPfs – Mounts an ftp/ssh/sftp/http/https server
- Loggedfs – Records all file access activity
- eCryptfs – Encrypts and decrypts data per file on the fly
- ROfs – a read only file system

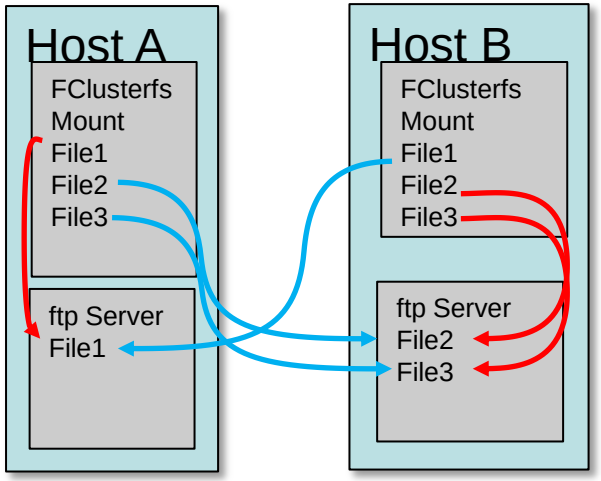
© University of South Wales

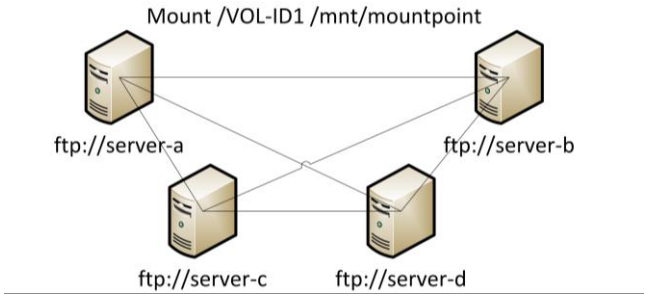
Distributed Data appearing as a single file system



© University of South Wales

FClusterfs





Remote Connection – Slower - Ethernet

Local Connection – Faster – SATA

RAM Connection – even faster – BUS speed!

```
fclusterfs
--mysql_user=me
--mysql_password=mypassword
--mysql_host=25.63.133.244
--mysql_database=fclusterfs
--volume=74a8f0f627cc0dc6
--audituser='Investigator Name'
/home/user/Desktop/fsmount
```


© University of South Wales

FClusterfs – MySQL Tables

inodes

inode	bigint(20) unsigned

fsfilename	varchar(1024)
inuse	int(11)
deleted	tinyint(4)
mode	int(11)
uid	int(10) unsigned
gid	int(10) unsigned
atime	int(10) unsigned
mtime	int(10) unsigned
ctime	int(10) unsigned
size	bigint(20)

© University of South Wales

Our Submission Information Package (SIP/DEB)

Header Section


```
<investigator>Nick Pringle</>
<case>A Villainous Crime</>
<date-time>12/May/2013 14:25:23</>
<description>This is a small 1GB memory stick taken from the desk of the suspect</><ScanStartedAt>Friday, November 29 2013. 13:42:52 GMT</>
<ThisFileScannedAt>Friday, November 29 2013. 13:42:52 GMT</>
<VolumeSerialNo>74a8f0f627cc0dc6</>
<VolumeLabel>My Label</>
<FileName>/mhash/lib/keygen_s2k.c</>
<NTFSDumpFileAttributes>
Dumping attribute $STANDARD_INFORMATION (0x10) from mft record 150 (0x96)
                    Resident:                                   Yes
                    Attribute flags:        0x0000
                     0x00
                    <FileAttributes> ARCHIVE (0x00000020)</>
Dumping attribute $FILE_NAME (0x30) from mft record 150 (0x96)
                    Resident:                                   Yes
                    Resident flags:                             0x01
                    Parent directory:       136 (0x88)
                    File Creation Time:     Sat Jul 20 18:25:53 2013 UTC
                    File Altered Time:      Sat Jul 20 18:25:53 2013 UTC
                    MFT Changed Time:       Sat Jul 20 18:25:53 2013 UTC
                    Last Accessed Time:     Sat Jul 20 18:25:53 2013 UTC
Dumping attribute $DATA (0x80) from mft record 150 (0x96)
                    Resident:                                   No
                    Attribute flags:        0x0000
                    Attribute instance:     2 (0x2)
                    Compression unit:       0 (0x0)
                    Actual Data size        6066 (0x17b2)</>
                    Allocated size:                             8192 (0x2000)
                    <<<Initialized size>>>: 6066 (0x17b2)
<TotalRuns>1</><Fragments>1</>
<run>1</><cluster1>242416</><sha1>A8724ACDB2135FE66EB7BE554CCF16091FBC2664</>
<run>1</><cluster2>242417</><sha1>D7A6B1A3F17E33A1F15BF8B815EC4B13410EFED3</>
<WholeFileSHA1>FC0198EF2F7782EF9EA8568853E6E3A48B86256D</>
<NTFSInodeGeneralInfo>
```


Data Section


```
<data>
begin-base64 777 FC0198EF2F7782EF9EA8568853E6E3A48B86256D.cpt
Dlevh4eFxd761tZ1zaPShNPDvGkB1FZn8UJiMY3zLCOAWKyj5CiPQSQOEGdU
KzhQCN3oG0Xh27lSyydHHwA7cCSeRS012Sv74NF16GixZ4f8qx7fMwtV73Ld
W9K53EwHUGnbHUw6WEOm0wh9ch8QvJcPcPvW3oIdQAA0HEBaB45I3XOaAr95
Yq37pBkMblDlC+/fu5ueFt6voIcPM9tD53GrO0G0T/6wAaPAqNEDWcCZTztj
bRH+FELEM9rxZidX8/glPd/UBXbgZ/IjSIsknIsZG+KMZhJg1AWxmniKj633
A0qeD/Fny9gj1i7f2RhCWrd78y2fXKt4YA/nM4osibDh1o9QsiGTjtrkdFM4
fy4rHA6w98UdIwvROiH+roMKx0twdiDgy+zlvgvSohF9PKMn5Nq7Y4KLw19k
p53JixBHilkoKefebVTybKNxNMh6c4QiNZucKQqRQWvVlYMgwqVbzqWiJQPM
5Mzhks7gDqZCx5s5QIl99w9fczGwurXn9yMjnNzGurFG32fo8ve/hoEAgsO6
slJ3/suViTtD+L97BrPqrsnkSv/gOr3aldEfstRgiA0A/v7ApAP6zDOe0TXD
HHZ3OkRfopu4HAy+k234k6HQRkvveoS2T53Jz6HrCSplAh2xqpMjRiTl5PF+
EpiHiyy3w8zX5oAgNMdkm/Nwv+CwESi8JnAbaCkcOEbiusNfjtxsF/SnaDPq
CzX2ezaKu9ElvLcqYDJA2ycQFw4MXy3Vr4gXNdg456Ael7nJbtfARZFrchg8
/bhN5itxLOda8/BjMlsA9zE9cXAPUM3W5bANniu75AXkbrI6yQDpsO5Kdf0Y
</data>
```


© University of South Wales

FClusterfs – MySQL Tables

VolumeListing

ID	bigint(20)
VolumeID	varchar(45)
FSRootInode	bigint(20)
keytext	varchar(1024)
ScanDateTime	char(27)
IssuedDateTime	datetime
ExpiresDateTime	datetime
Device	varchar(45)

serveraccessinfo

ID	int(11)
Protocol	varchar(45)
IP	varchar(45)
User	varchar(45)
Password	**varchar(45)**

inodes

inode	bigint(20) unsigned
VolumeID	varchar(45)
fsfilename	varchar(1024)
inuse	int(11)
deleted	tinyint(4)
mode	int(11)
uid	int(10) unsigned
gid	int(10) unsigned
atime	int(10) unsigned
mtime	int(10) unsigned
ctime	int(10) unsigned
size	bigint(20)
SHA1	varchar(40)
originallocation	varchar(1024)
firststorageprotocol	varchar(10)
firststorageserver	varchar(45)
firststoragefilename	varchar(1024)
firststorageinplace	tinyint(4)
firststoragearrivaldatetime	datetime
[illegible]	[illegible]

tree

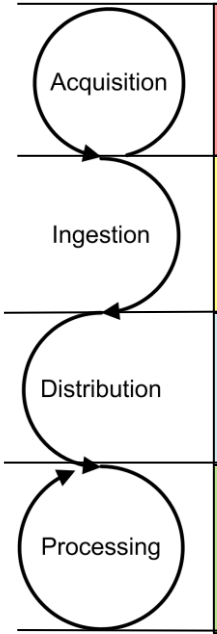
inode	bigint(20) unsigned
VolumeID	char(45)
parent	int(10) unsigned
name	varchar(255)

metadata

inode	bigint(20)
metadata	longtext
VolumeID	varchar(45)

© University of South Wales

FCluster Architecture
Roles and Zones

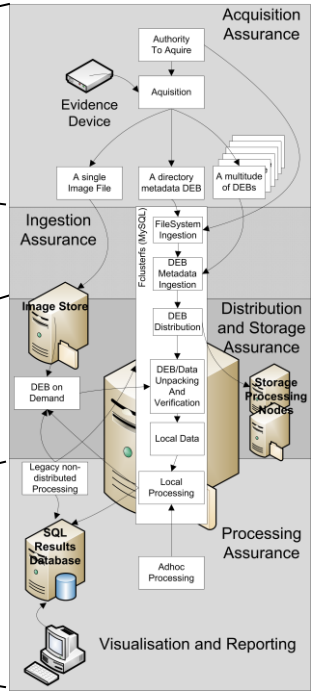


- Acquisition Authority
- Imager

- FClusterfs metadata storage
- Metadata Import/Load Balancer

- Replicator
- Data Storage Server

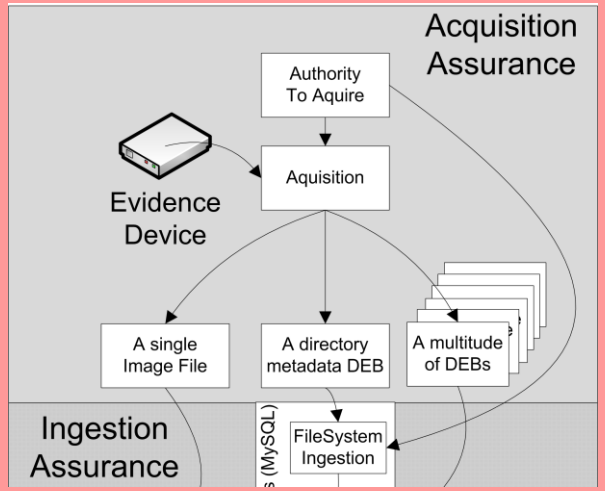
- Processing Server
- Results Meta Data table



© University of South Wales

Assurance Zones – Acquisition - Overview

1. The cluster issues an "authority to image". This includes a "one time use" key to be used to encrypt the evidence.
2. The imaging device creates the image, SIP/DEB of the file directory and SIP/DEBs of the file data which are encrypted using the one time use key.
3. SIP/DEBs are pushed/pulled to the cluster



© University of South Wales

Assurance Zones – Acquisition – Detail 1 of 6

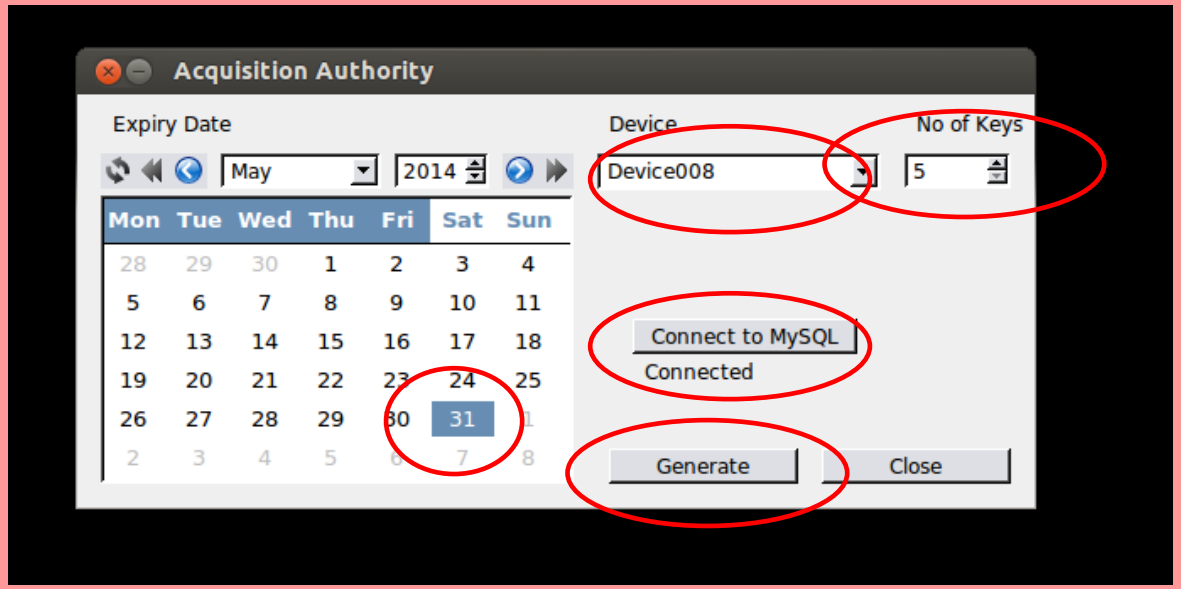
VolumeListing × | inodes × | tree × | serveraccessinfo × | audit × | nodestate ×

Filter: | Edit: | Export: | Autosize:

#	ID	Device	IssuedDateTime	ExpiresDateTime	ScanDateTime	VolumeID	FSRootInode	keytext
1	193	Device003	2014-04-17 14:44:00	2014-04-30 00:00:00			0	qBf&fCd7HN+59otg13rBkq+t=%I2Kk9tv7y
2	194	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	%0OI-U2CU4c)7lUSv(Cin4+0QQSx8MVFwFE
3	196	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	HJ7(qGMUxygF9xzsgv$!^e27uIREg%f#kXS
4	197	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00	2014-04-18 19:19:43 +00:00	74a8f0f627cc0dc6	3365	Xt(VWtO2OXLH=j0P2Afd5qQQeH*V(d)Dmg!
5	198	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00	2014-04-18 21:25:28 +00:00	1c0376672b6c06d3	451	c8R$GBvBI*=Ve11Oe^fpAPI!aOzLY6mgMK=
6	199	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	rem!ET4i(dHuqzkHl4QkjeI901TuV5Q7UavP^
7	200	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	StTTo$#(q3VELyS%maXRq4p441b)S#+fGS
8	201	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00	2014-04-18 20:20:56 +00:00	6449bf4a176afd35	3168	Iv#6o^N447U+#ymTL91Du$GSz=%=!Yan
9	202	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	BMaz1a6objqq_U==WB+5B7$hgr*Oz3j1$z
10	203	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00	2014-04-18 21:21:20 +00:00	23ba7f8e25ef0f52	1154	*%MU5)9CRD5azoAI3tU_VX=!Nw4kLQsv+e
11	208	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	%E=$sfR6KW34Gmul=6P0EkNcrS8_qk^PIC
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

© University of South Wales

Assurance Zones – Acquisition – Detail 2 of 6



© University of South Wales

Assurance Zones – Acquisition – Detail 3 of 6

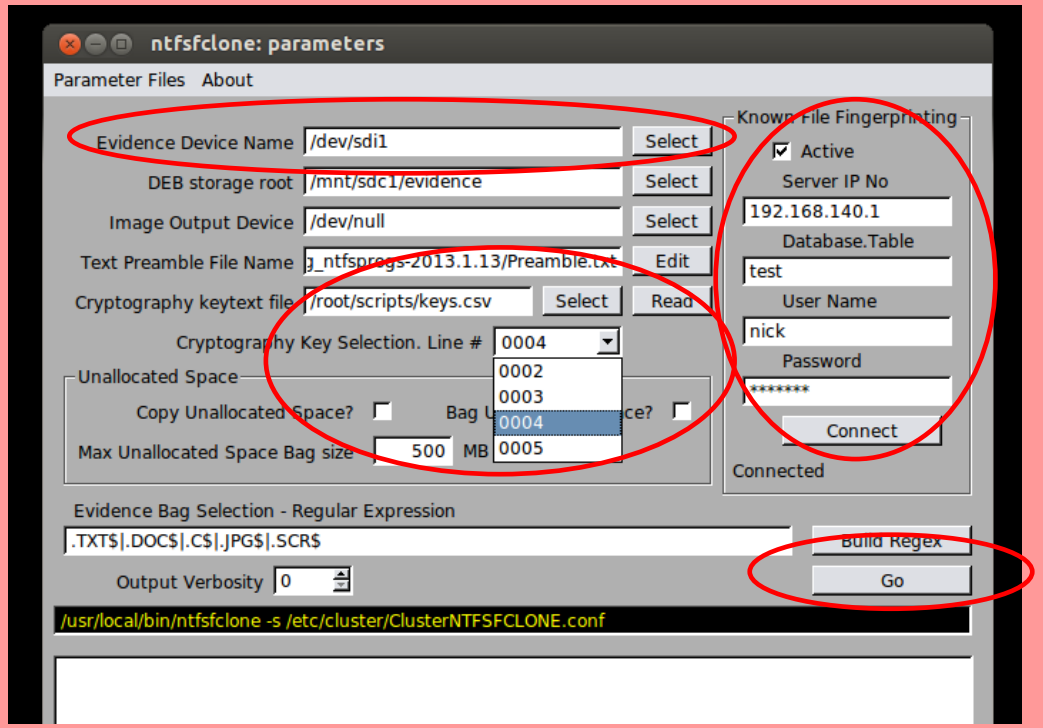
VolumeListing × | inodes × | tree × | serveraccessinfo × | audit × | nodestate ×

Filter: Edit: Export: Autosize:

#	ID	Device	IssuedDateTime	ExpiresDateTime	ScanDateTime	VolumeID	FSRootInode	keytext
1	193	Device003	2014-04-17 14:44:00	2014-04-30 00:00:00			0	qBf&fCd7HN+59otg13rBkq+t=%I2Kk9tv7y
2	194	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	%0Ol-U2CU4c)7lUSv(Cin4+0QQSx8MVFwF8
3	196	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	HJ7(qGMUxygF9xzsgv$!^e27uIREg%f#kXS
4	197	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00	2014-04-18 19:19:43 +00:00	74a8f0f627cc0dc6	3365	Xt(VWtO2OXLH=j0P2Afd5qQQeH*V(d)Dmg!
5	198	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00	2014-04-18 21:25:28 +00:00	1c0376672b6c06d3	451	c8R$GBvBI*=Ve11Oe^fpAPI!aOzLY6mgMK=
6	199	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	rem!ET4i(dHuqzkHl4QkjeI901TuV5Q7UavP^
7	200	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	StTTo$#(q3VELyS%maXRq4p441b)S#+fGS
8	201	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00	2014-04-18 20:20:56 +00:00	6449bf4a176afd35	3168	Iv#6o^N447U+#ymTL91Du$GSz=%=!Yan
9	202	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	BMaz1a6objqq_U==WB+5B7$hgr*Oz3j1$z
10	203	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00	2014-04-18 21:21:20 +00:00	23ba7f8e25ef0f52	1154	*%MU5)9CRD5azoAI3tU_VX=!Nw4kLQsv+e
11	208	Device006	2014-04-17 16:48:00	2014-05-31 00:00:00			0	[illegible]
12	253	Device008	2014-04-21 20:41:00	2014-05-31 00:00:00	NULL		NULL	4S2g29lPUoO2p2lVhn[illegible]AE+pNIB$*
13	254	Device008	2014-04-21 20:41:00	2014-05-31 00:00:00	NULL		NULL	Rd5+VNJrXHztcR6w*z54DYIYUjQNH!kF[illegible]
14	255	Device008	2014-04-21 20:41:00	2014-05-31 00:00:00	NULL		NULL	dw)s=jmro!26j^6iL5z3fkPkNtzcfrsn^MopW
15	256	Device008	2014-04-21 20:41:00	2014-05-31 00:00:00	NULL		NULL	7p8WuYTC0m2h2%5Rxid5^wFOqT)CV=5v
16	257	Device008	2014-04-21 20:41:00	2014-05-31 00:00:00	NULL		NULL	b6q^P+AgUT^90_lwnRyT4aMuUq%%C$dw
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

© University of South Wales

Assurance Zones – Acquisition – Detail 4 of 6



© University of South Wales

Assurance Zones – Acquisition – Detail 5 of 6

```
Please wait. Reading the whole directory Structure
NTFS volume version: 3.1
Serial No is [6786b2132b5822fb]
Volume Name is []
Input Volume Cluster size      : 4096 bytes
Current input volume size: 1072689152 bytes (1073 MB)
Current device size: 1072693248 bytes (1073 MB)
header mkdir /mnt/sdc1/evidence
header mkdir /mnt/sdc1/evidence/6786b2132b5822fb
Saving volume metadata. mv /mnt/sdc1/evidence/volume.meta /mnt/sdc1/evidence/6786b2132b5822fb/6786b2132b5822fb-filesystem.meta
NTFS Size 1072689152,   261887 Clusters of     4096 bytes
RegexWantedExtensions are .TXT$|.DOC$|.C$|.JPG$|.SCR$
Scanning volume ...
     9 candidate evidence items from      124 in total.
Copying high value targets
     1 of      9, File Name [/Videos etc],     8192 bytes long.       2 whole clusters and       0 bytes.Encrypting, uuencoding and packing into meta. Saved
     2 of      9, File Name [/Videos etc/Version PC-3000 and DE.txt],     9153 bytes long.       2 whole clusters and     961 bytes.Encrypting, uuencoding and packing into meta. Saved
     3 of      9, File Name [/Picture 003.jpg],  3679659 bytes long.     898 whole clusters and    1451 bytes.Encrypting, uuencoding and packing into meta. Saved
     4 of      9, File Name [/Picture 002.jpg],  3646873 bytes long.     890 whole clusters and    1433 bytes.Encrypting, uuencoding and packing into meta. Saved
     5 of      9, File Name [/Deepspar Data Recovery Course.doc],   160768 bytes long.      39 whole clusters and    1024 bytes.Encrypting, uuencoding and packing into meta. Saved
     6 of      9, File Name [/Ace Contract.doc],   105984 bytes long.      25 whole clusters and    3584 bytes.Encrypting, uuencoding and packing into meta. Saved
     7 of      9, File Name [/185552-500-375.jpg],    44234 bytes long.      10 whole clusters and    3274 bytes.Encrypting, uuencoding and packing into meta. Saved
     8 of      9, File Name [/186153-500-375.jpg],    43611 bytes long.      10 whole clusters and    2651 bytes.Encrypting, uuencoding and packing into meta. Saved
     9 of      9, File Name [/185553-500-375.jpg],    41729 bytes long.      10 whole clusters and     769 bytes.Encrypting, uuencoding and packing into meta. Saved
     1 of    115, File Name [/$MFT], not selected as evidence.
     2 of    115, File Name [/$MFTMirr], not selected as evidence.
     3 of    115, File Name [/$LogFile], not selected as evidence.
     4 of    115, File Name [/$Volume], not selected as evidence.
     5 of    115, File Name [/$AttrDef], not selected as evidence.
     6 of    115, File Name [/.], not selected as evidence.
     7 of    115, File Name [/$Bitmap], not selected as evidence.
```

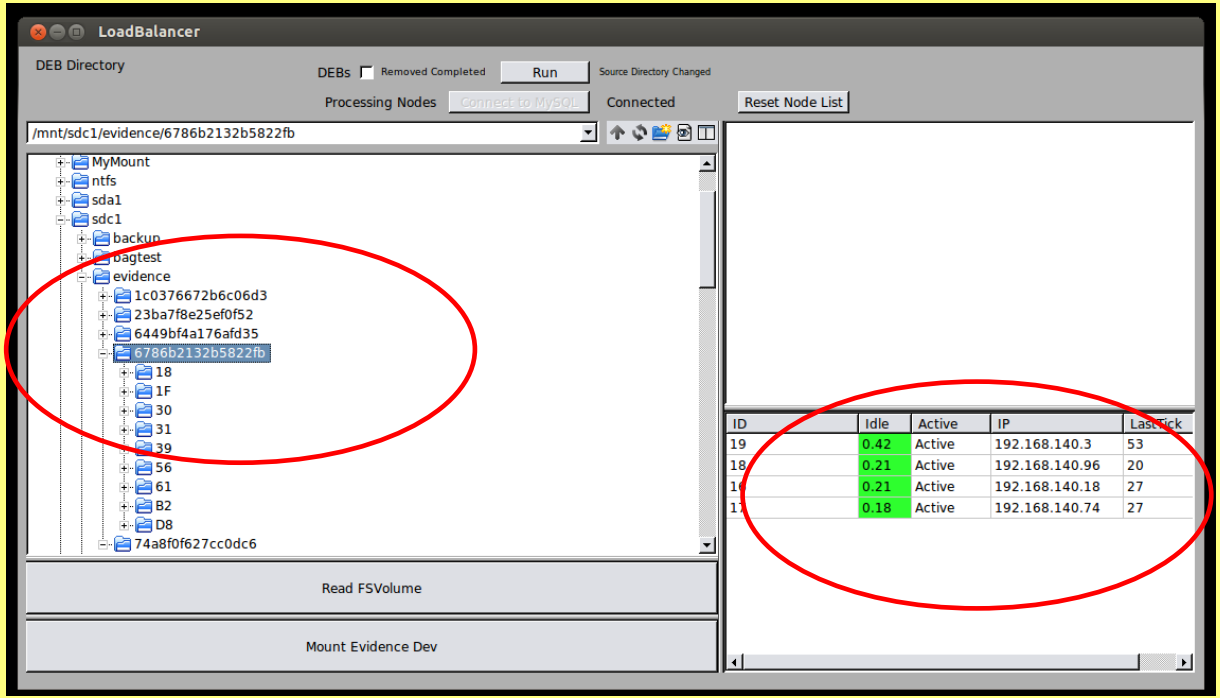

© University of South Wales

Assurance Zones – Acquisition – Detail 6 of 6

```
root@ubuntu:/mnt/sdc1/evidence# tree 23ba7f8e25ef0f52
23ba7f8e25ef0f52
├── 00
│   ├── 23ba7f8e25ef0f52-001D9EE55046AFC205CF15B81E2537BB392C7EB6.meta
│   ├── 23ba7f8e25ef0f52-00464C159732F0386C73EB6D26E16E07A9EFBBCA.meta
│   └── 23ba7f8e25ef0f52-00E7DA8F157ABD94A266A115B96D621FE14BA66A.meta
├── 01
│   ├── 23ba7f8e25ef0f52-01260BAD52E8EBE7E78A8C1E1714FBD5A515C46D.meta
│   ├── 23ba7f8e25ef0f52-016EE6BEE65E543D08296E2DFE0BCDAAD99B87BE.meta
│   └── 23ba7f8e25ef0f52-017E148DE26F4A0580399788A4F064E4D6B13713.meta
├── 02
│   ├── 23ba7f8e25ef0f52-026D05CD2DC77976D1EA8BAAF17E069DFF92356A.meta
│   └── 23ba7f8e25ef0f52-02F99EAB961BF330405770404ED21BBF05D512C7.meta
├── 03
│   ├── 23ba7f8e25ef0f52-033267D0363B50754425E0153DB8312B2C2E5999.meta
│   └── 23ba7f8e25ef0f52-03E7F306D937DFD991A059337683A11321456066.meta
├── 04
│   ├── 23ba7f8e25ef0f52-04C7F95EF38A66858AB56E386D4E1F7B8025548B.meta
│   ├── 23ba7f8e25ef0f52-04C9E5EE4125175E412CBD4849C7FD6A44A5BB0A.meta
│   ├── 23ba7f8e25ef0f52-04D0A247443DDAEDBB6F970FC36BC7B430B226EC.meta
│   └── 23ba7f8e25ef0f52-04DD028B2DFFBF04034811615C1DA3AB7DCF2BDE.meta
├── 05
│   └── 23ba7f8e25ef0f52-05BFFC3543078E15208DCA467792223FA6442B41.meta
├── 06
│   ├── 23ba7f8e25ef0f52-0600BBA2ED5CF7D3326938F87B29702D575640A3.meta
│   ├── 23ba7f8e25ef0f52-060ED32C4092FA3BC067C51C73CCB09DCAA9F922.meta
```

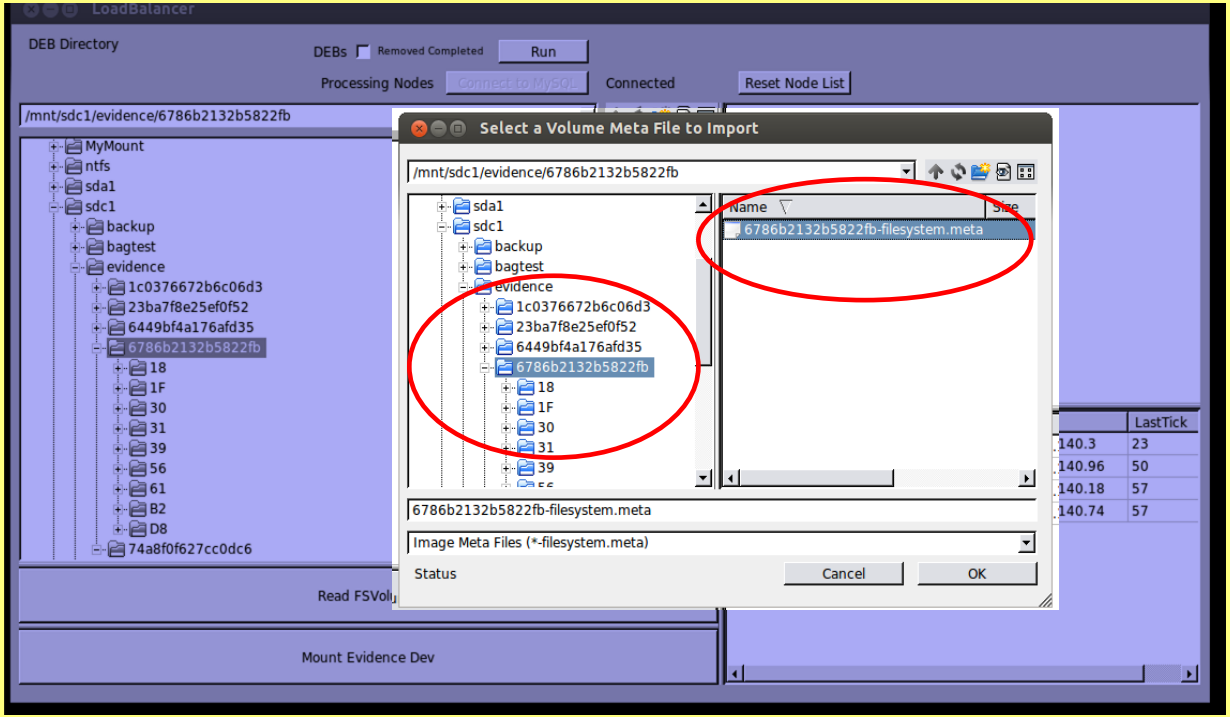

© University of South Wales

Assurance Zones – Metadata Import – Detail 1 of 6



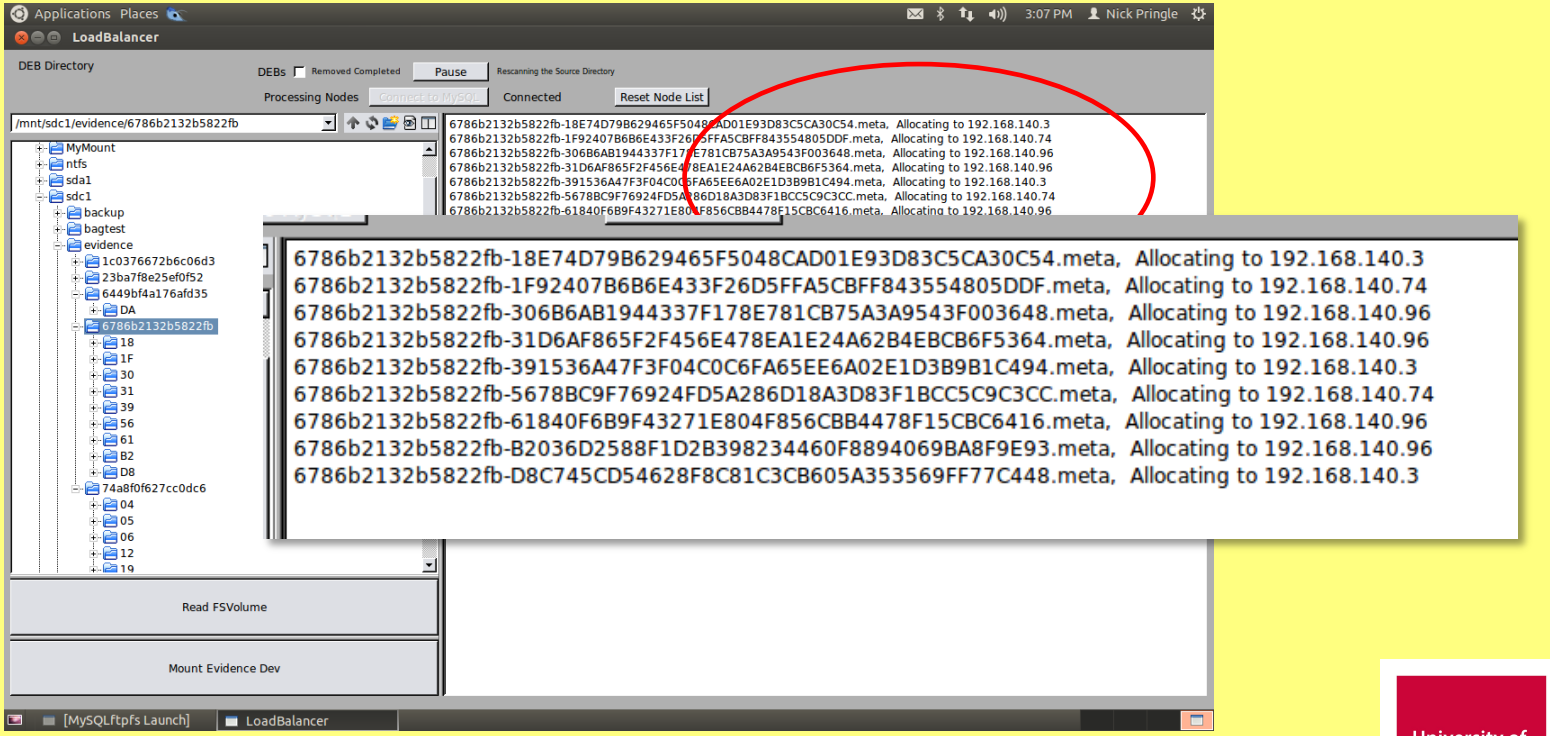
© University of South Wales

Assurance Zones – Metadata Import – Detail 2 of 6



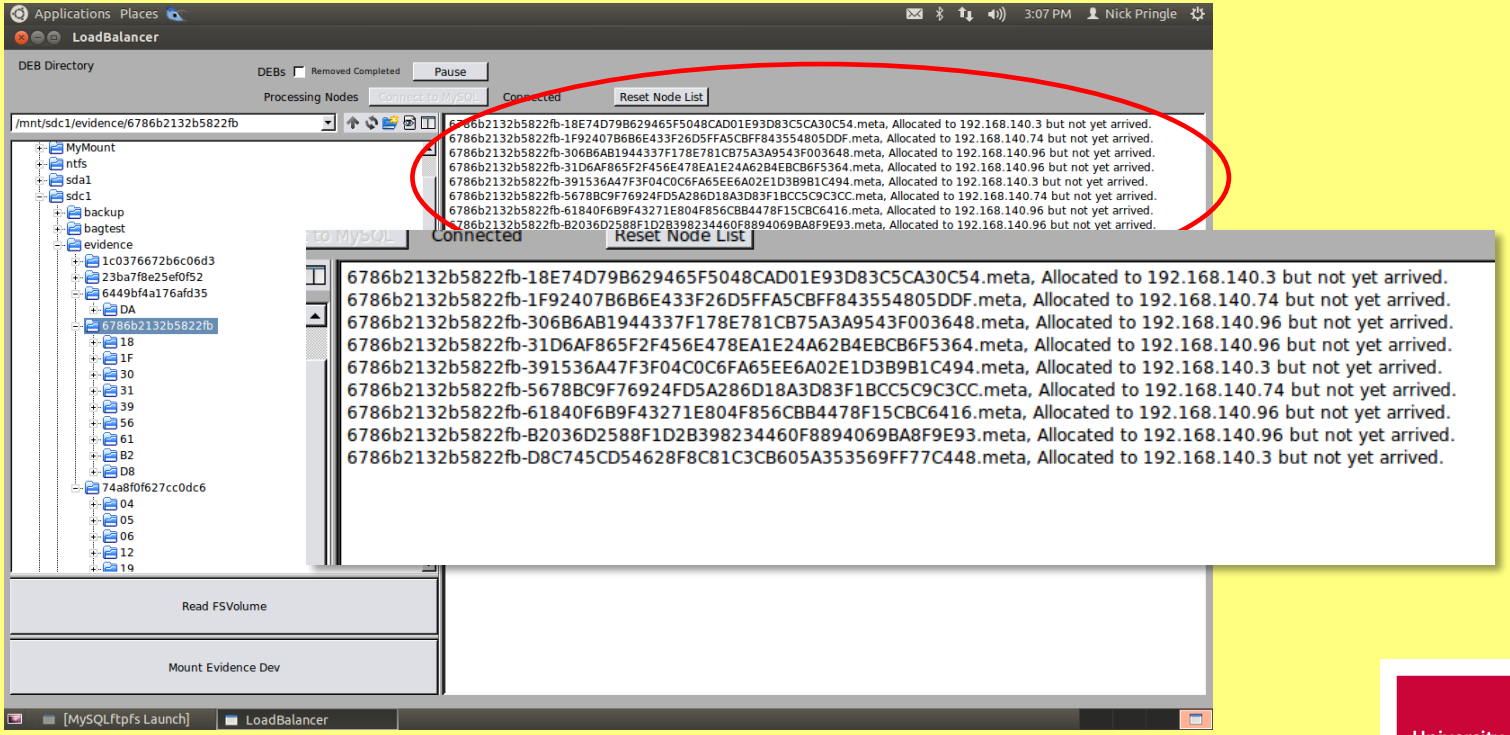
© University of South Wales

Assurance Zones – Metadata Import – Detail 3 of 6



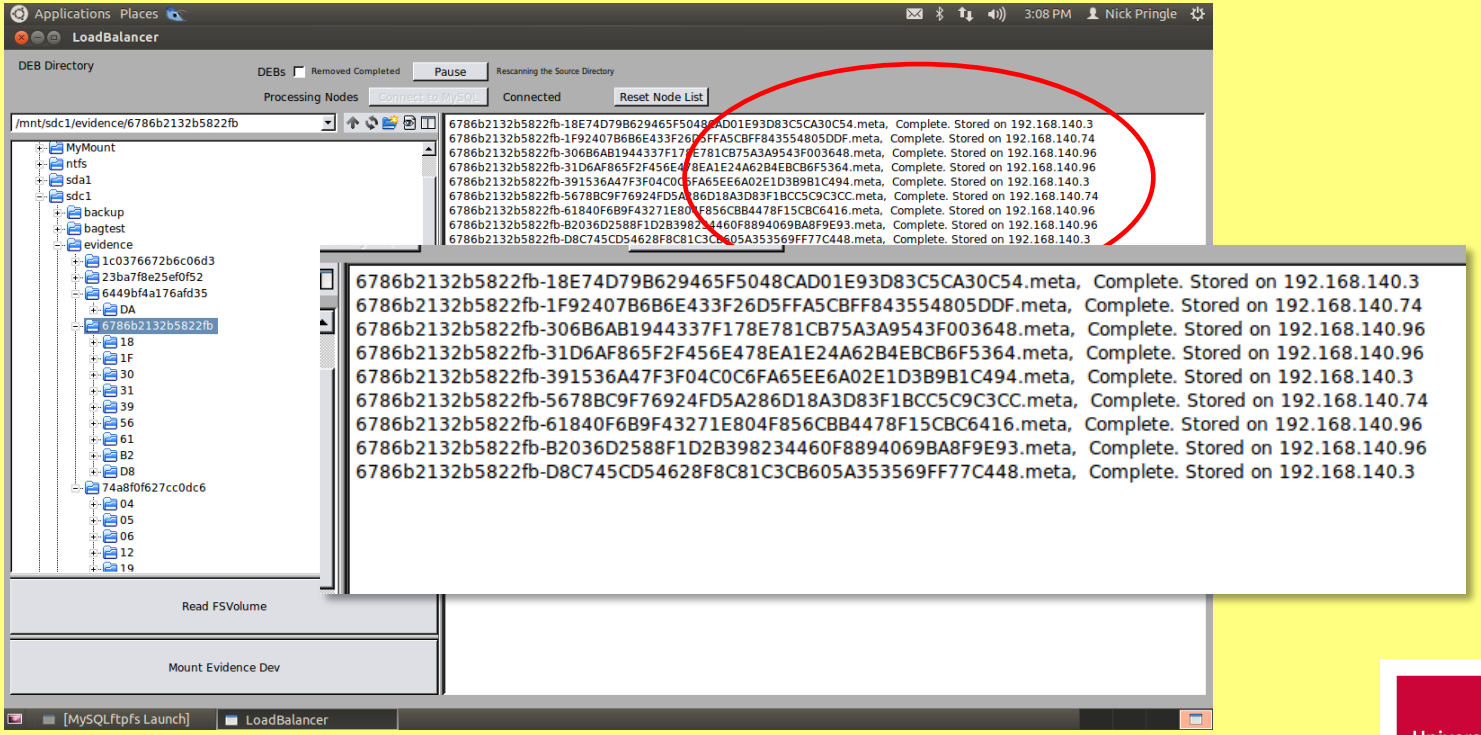
© University of South Wales

Assurance Zones – Metadata Import – Detail 4 of 6



© University of South Wales

Assurance Zones – Metadata Import – Detail 5 of 6



© University of South Wales

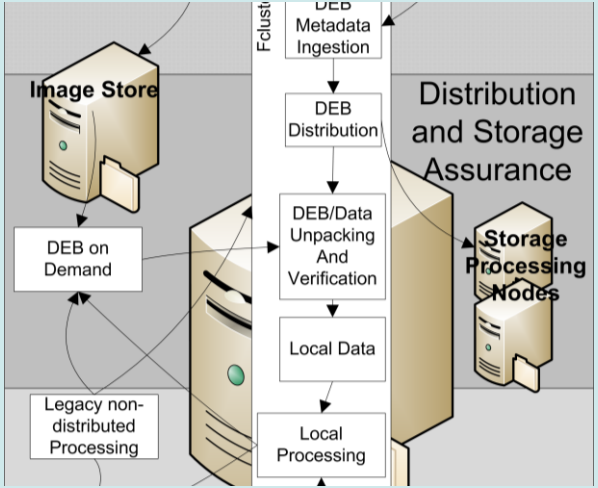
Assurance Zones – Metadata Import – Detail 6 of 6

secondstoragelastvalidated	thirdstorageprotocol	thirdstorageserver	thirdstoragefilename	thirdstorageinplace	thirdstoragearrivaldatetime	thirdstorageunpacked
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	ftp	192.168.140.3	6d13a60005e973e5-55817B0CB6794938961C0CEF1D75794684B984EC	1	2014-04-28 15:01:36	1
NULL	ftp	192.168.140.13	unknown	NULL	NULL	NULL
NULL	ftp	192.168.140.96	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	ftp	192.168.140.13	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	ftp	192.168.140.74	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL
NULL	unknown	unknown	unknown	NULL	NULL	NULL

© University of South Wales

Assurance Zones – Distribution - Overview

1. Each SIP/DEB is read and only if it is expected, ie found in the inodes table, it is copied to the location as recorded in the inode table
2. The SIP is unpacked, decrypted and header data added to the meta-data table
3. The inodes table is updated with the storage data status
4. In due course, the SIP/DEB will be replicated to 2 other locations and the inodes table updated accordingly.



© University of South Wales

Assurance Zones – Distribution – Detail 1 of 2

VolumeListing × | inodes × | tree × | serveraccessinfo × | audit × | nodestate × | SQL File 3* × | Query 12 ×

Filter: | Edit: | Export: | Autosize: | Fetch rows:

inode	VolumeID	fsfilename	inuse	deleted	mode	uid	gid	atime	mtime	ctime	size	SHA1
3459	74a8f0f627cc0dc6	/mhash/lib/CVS/Repository	0	0	33204	65534	65534	1374274800	1374274800	1374274800	10	NULL
3460	74a8f0f627cc0dc6	/mhash/lib/CVS/Root	0	0	33204	65534	65534	1374274800	1374274800	1374274800	47	NULL
3461	74a8f0f627cc0dc6	/mhash/lib/CVS/x	0	0	33204	65534	65534	1374274800	1374274800	1374274800	0	NULL
3462	74a8f0f627cc0dc6	/mhash/lib/gosthash.c	0	0	33204	65534	65534	1374274800	1374274800	1374274800	22776	95F5E9809083A66
3463	74a8f0f627cc0dc6	/mhash/lib/haval.c	0	0	33204	65534	65534	1374274800	1374274800	1374274800	54223	533919251DEAAF2

originallocation	firststorageprotocol	firststorageserver	firststoragefilename	firststorageinplace	firststoragea
NULL	unknown	unknown	unknown	0	NULL
NULL	unknown	unknown	unknown	0	NULL
NULL	unknown	unknown	unknown	0	NULL
9E /192.168.140.3/mnt/sdc1/evidence/74a8f0f627cc0dc6/95	ftp	192.168.140.18	74a8f0f627cc0dc6-95F5E9809083A66BE0063EAE0C194905969D7E9E	1	2014-04-18
57 /192.168.140.3/mnt/sdc1/evidence/74a8f0f627cc0dc6/53	ftp	192.168.140.3	74a8f0f627cc0dc6-533919251DEAAF2D9E9CC892C40EF7915A3A7E57	1	2014-04-18
8B /192.168.140.3/mnt/sdc1/evidence/74a8f0f627cc0dc6/85	ftp	192.168.140.74	74a8f0f627cc0dc6-8519C83381BC58AE417758EEBC51B685574C0E8B	1	2014-04-18

tvalidated	secondstorageprotocol	secondstorageserver	secondstoragefilename	secondstorageinplace	secondstoragearrivaldatetime	secondstorageunpacked	s
	unknown	unknown	unknown	NULL	NULL	NULL	NU
	unknown	unknown	unknown	NULL	NULL	NULL	NU
	unknown	unknown	unknown	NULL	NULL	NULL	NU
	ftp	192.168.140.74	74a8f0f627cc0dc6-95F5E9809083A66BE0063EAE0C194905969D7E9E	1	2014-04-18 19:29:33	1	NU
	ftp	192.168.140.3	74a8f0f627cc0dc6-533919251DEAAF2D9E9CC892C40EF7915A3A7E57	1	2014-04-18 19:29:33	1	NU

ed	thirdstorageprotocol	thirdstorageserver	thirdstoragefilename	thirdstorageinplace	thirdstoragearrivaldatetime	thirdstorageunpacked	thirdstoragelastvalid
	unknown	unknown	unknown	NULL	NULL	NULL	NULL
	unknown	unknown	unknown	NULL	NULL	NULL	NULL
	unknown	unknown	unknown	NULL	NULL	NULL	NULL
	ftp	192.168.140.18	74a8f0f627cc0dc6-95F5E9809083A66BE0063EAE0C194905969D7E9E	1	2014-04-18 19:29:33	1	NULL
	ftp	192.168.140.3	74a8f0f627cc0dc6-533919251DEAAF2D9E9CC892C40EF7915A3A7E57	1	2014-04-18 19:29:33	1	NULL

© University of South Wales

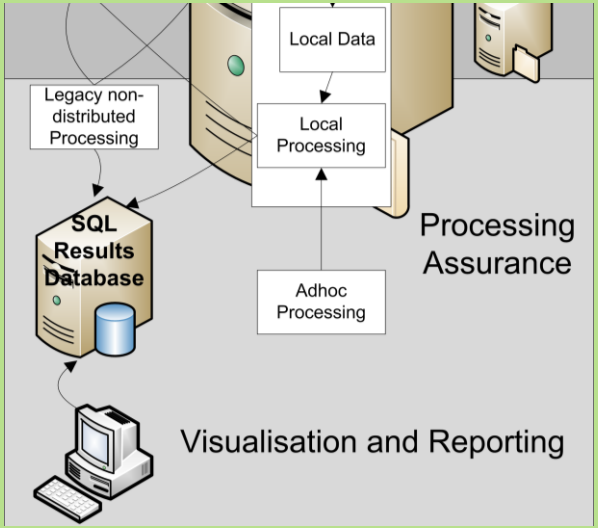
Assurance Zones – Distribution – Detail 2 of 2

#	inode	metadata	VolumeID	result1	result2
34	2698	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</> <description>This is a small 1GB memory stick taken from the desk of the suspect</> <ThisFileScannedAt>Frida...	23ba7f8e25ef0f52	NULL	NULL
35	2699	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</> <description>This is a small 1GB memory stick taken from the desk of the suspect</> <ThisFileScannedAt>Frida...	23ba7f8e25ef0f52	NULL	NULL
36	2700	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</> <description>This is a small 1GB memory stick taken from the desk of the suspect</> <ThisFileScannedAt>Frida...	23ba7f8e25ef0f52	NULL	NULL
37	2701	none yet	NULL	NULL	NULL
38	2702	none yet	NULL	NULL	NULL
39	2703	none yet	NULL	NULL	NULL
40	2704	none yet	NULL	NULL	NULL
41	2705	none yet	NULL	NULL	NULL
42	2706	none yet	NULL	NULL	NULL
43	2707	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</> <description>This is a small 1GB memory stick taken from the desk of the suspect</> <ThisFileScannedAt>Frida...	23ba7f8e25ef0f52	NULL	NULL
44	2708	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</>	23ba7f8e25ef0f52	NULL	NULL

© University of South Wales

Assurance Zones – Processing - Overview

1. Using the processing table, a standard set of tasks is run on the data stored locally on the host
2. Results are usually recorded as XML formatted data in the results table within the same database referenced by inode number.



© University of South Wales

Assurance Zones – Processing – Detail 1 of 1

Filter: Edit: Export: Autosize: Fetch rows:

#	inode	metadata	VolumeID	result1	result2
1	2665	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</> <description>This is a small 1GB memory stick taken from the desk of the suspect</> <ThisFileScannedAt>Frida...	23ba7f8e25ef0f52	----------+---------- Tag |Value ----------+---------- Manufacturer |FUJIFILM Model |FinePix S5700 S	
2	2666	none yet	NULL	NULL	NULL
3	2667	none yet			
4	2668	none yet			
5	2669	none yet			
6	2670	none yet			
7	2671	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</> <description>This is a small 1GB mem <ThisFileScannedAt>Frida...			
8	2672	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</> <description>This is a small 1GB mem <ThisFileScannedAt>Frida...			
9	2673	none yet			
10	2674	<investigator>Nick Pringle</> <case>A Villainous Crime</> <date-time>12/May/2013 14:25:23</> <description>This is a small 1GB mem <ThisFileScannedAt>Frida...			
		<investigator>Nick Pringle</> <case>A Villainous Crime</>			

23ba7f8e25ef0f52	Tag |Value ----------+---------- Manufacturer |FUJIFILM Model |FinePix S5700 S	NULL
23ba7f8e25ef0f52	----------+---------- Tag |Value ----------+---------- Manufacturer |FUJIFILM Model |FinePix S5700 S	NULL
NULL	NULL	NULL
23ba7f8e25ef0f52	not JPG	NULL

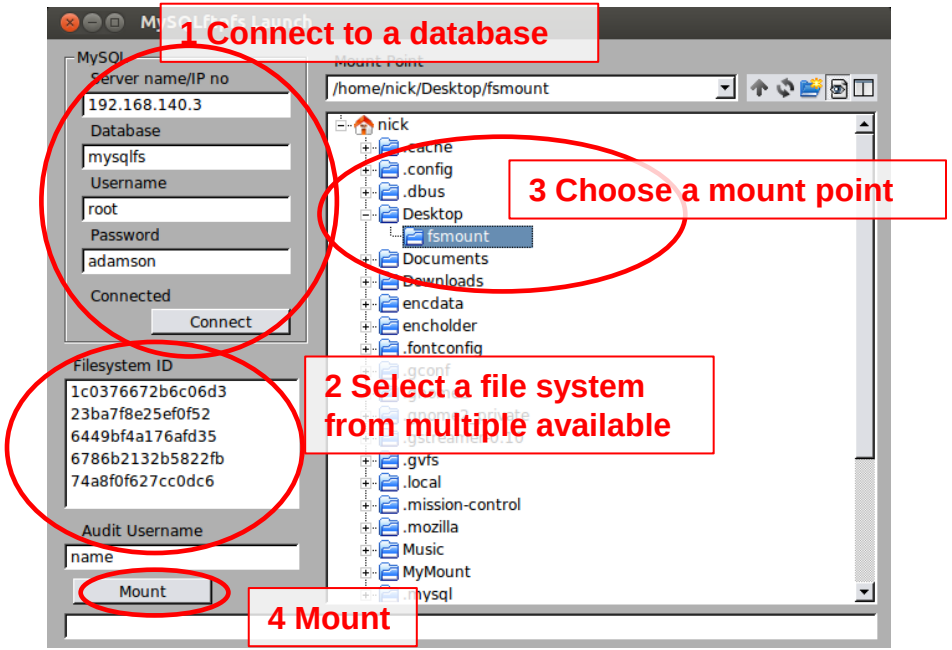
INFORMATIONSECURITY RESEARCHGROUP
© University of South Wales
University of South Wales Prifysgol De Cymru

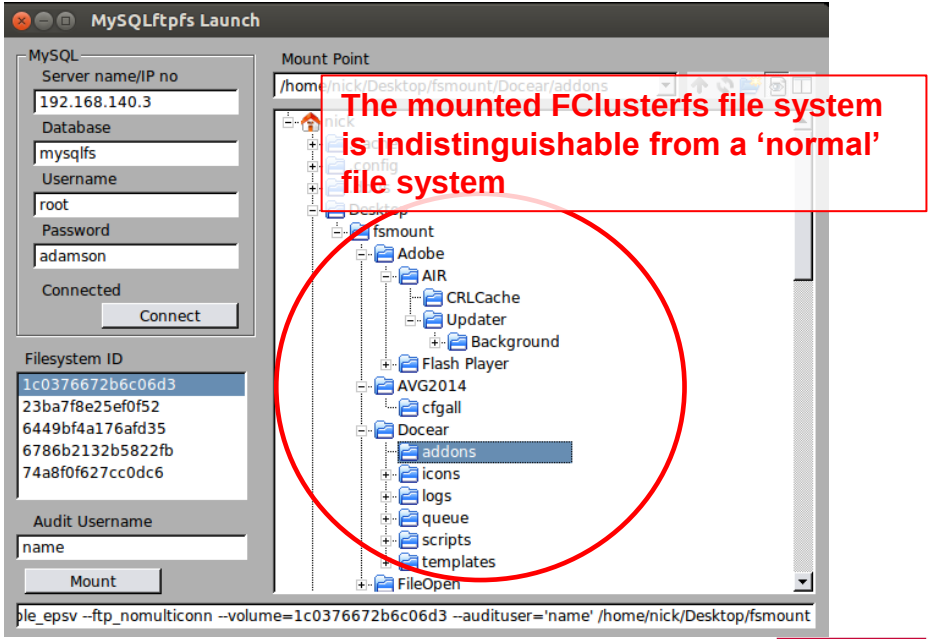
Audit

#	ID	DateTime	Investigator	Action	inode
749	2894	2014-04-18 19:27:30.713169324 +01:00	unpackfiles script	DEB unpack	1234
750	2895	2014-04-18 19:27:30.779951455 +01:00	movefiles script	DEB move	2692
751	2896	2014-04-18 19:27:30.896467988 +01:00	movefiles script	DEB move	2693
752	2897	2014-04-18 19:27:31.023123067 +01:00	movefiles script	DEB move	2696
753	2898	2014-04-18 19:27:31.155038482 +01:00	movefiles script	DEB move	2697
754	2899	2014-04-18 19:27:31.297371802 +01:00	unpackfiles script	DEB unpack	1241
755	2900	2014-04-18 19:27:31.338570715 +01:00	movefiles script	DEB move	2698
756	2901	2014-04-18 19:27:31.477117381 +01:00	movefiles script	DEB move	2699
757	2902	2014-04-18 19:27:28.790614283 +01:00	unpackfiles script	DEB unpack	1589
758	2903	2014-04-18 19:27:31.606249551 +01:00	movefiles script	DEB move	2700
759	2904	2014-04-18 19:27:31.690205399 +01:00	unpackfiles script	DEB unpack	1245
760	2905	2014-04-18 19:27:31.725864080 +01:00	movefiles script	DEB move	2707
761	2906	2014-04-18 19:27:31.854338524 +01:00	movefiles script	DEB move	2708
762	2907	2014-04-18 19:27:29.221416118 +01:00	unpackfiles script	DEB unpack	1591

© University of South Wales

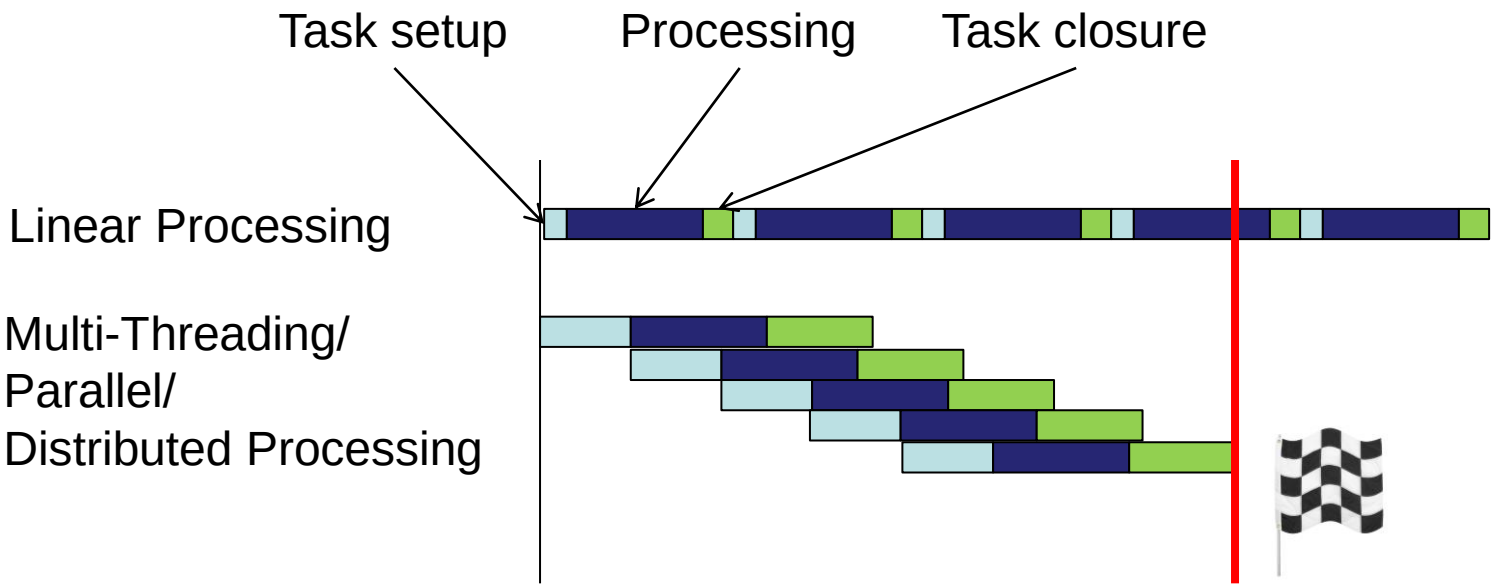
Mounting the file system





© University of South Wales

Latency and Multi-threading and Parallel Processing



INFORMATIONSECURITY RESEARCHGROUP
© University of South Wales
University of South Wales
Prifysgol De Cymru

Why is this the right approach?

- This could be achieved within an application program but each package would to implement it and gain approval.
- Working at file system level the efficacy is global
- Interaction with FClusterfs is unavoidable
- Fclusterfs controls data access and maintains Assurance

© University of South Wales

In Summary

- Distributed processing is a prime candidate to reduce the backlog but there are problems
- We lose ‘the image’; one of the foundations that has evolved in digital forensics over the last 20 years
- We can replace it by learning from, not adopting, Hadoop

© University of South Wales

Funded by…

ESF

Llywodraeth Cymru
Welsh Government

Ewrop & Chymru: Buddsoddi yn eich dyfodol
Cronfa Gymdeithasol Ewrop

Europe & Wales: Investing in your future
European Social Fund

kess

Ysgoloriaethau Sgiliau Economi Gwybodaeth
Knowledge Economy Skills Scholarships

© University of South Wales

Information Assurance in a Distributed Forensic Cluster

Questions?

© University of South Wales