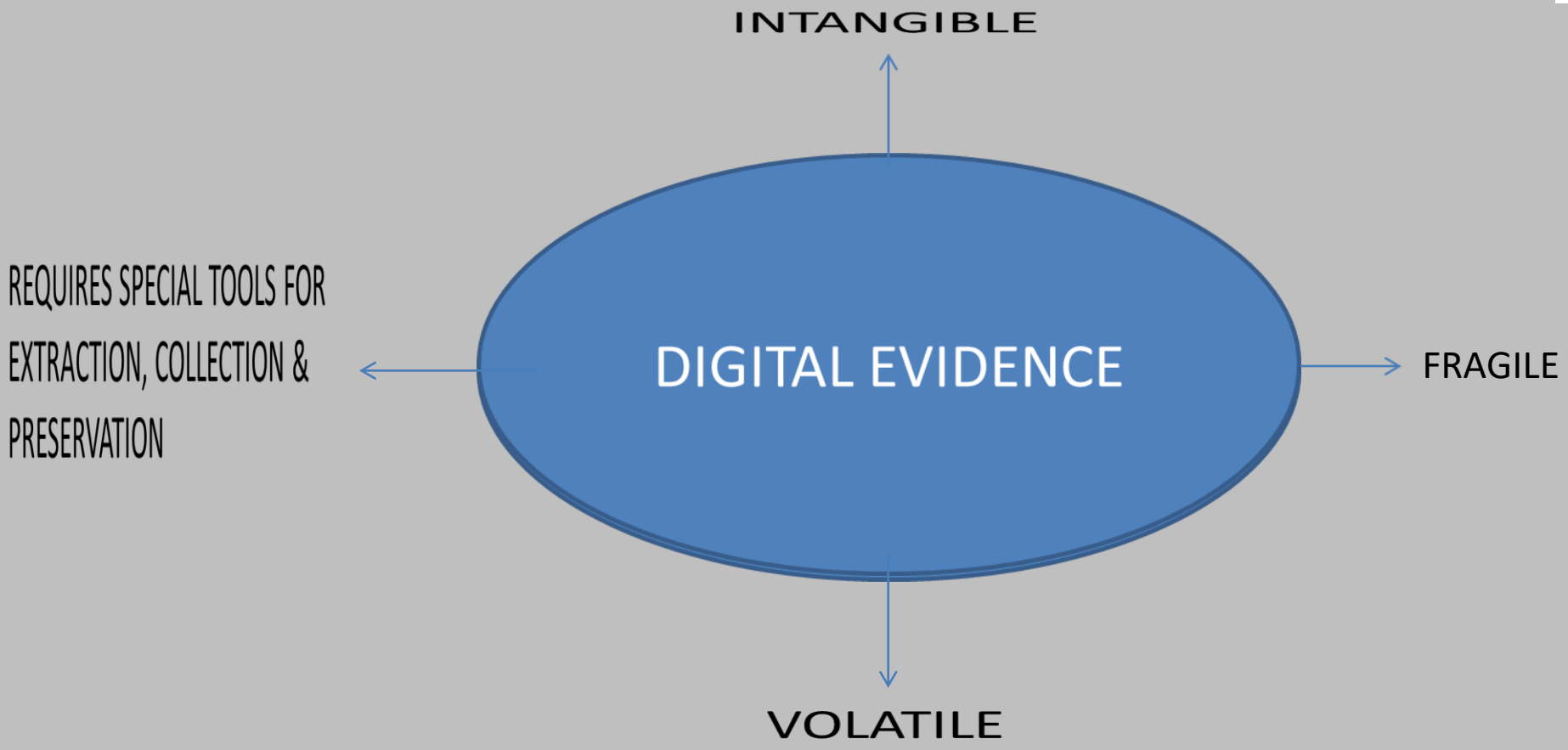
Nuances of Digital Evidence

Justice Raja Vijayaraghavan,

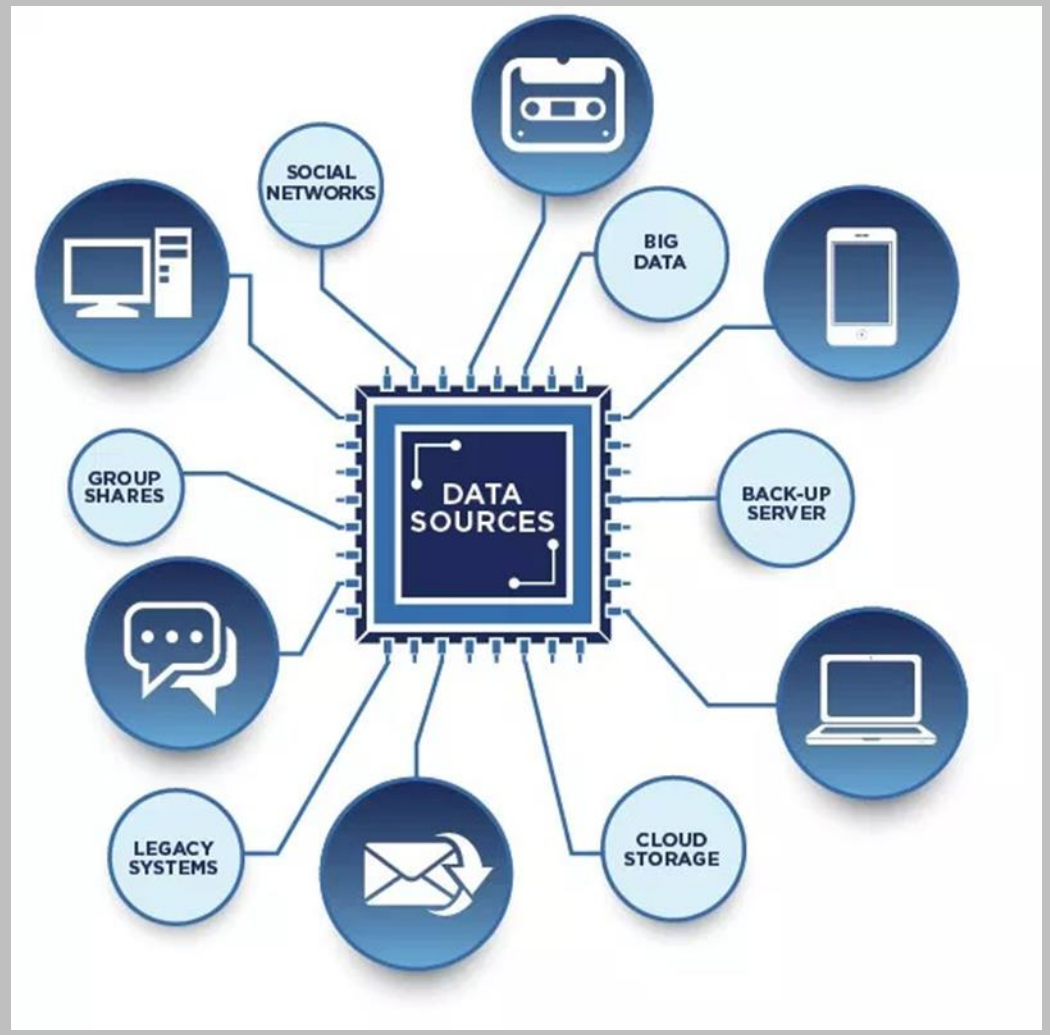
High Court of Kerala,

Workshop on Digital Evidence,
September 2019

Uniqueness of Digital Evidence



Types of Digital Evidence



Traditional data sources for electronic evidence

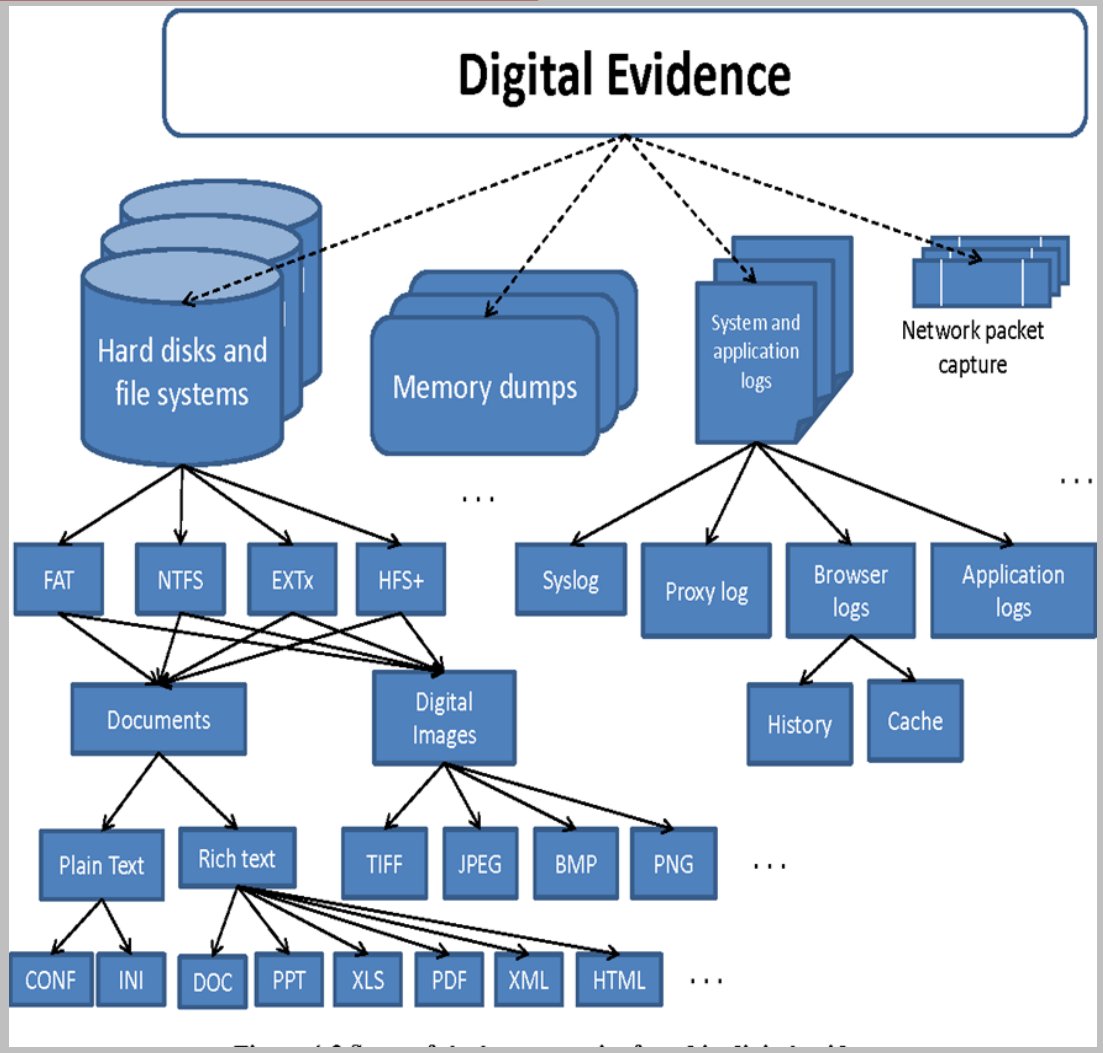
- Desktop computers
- Laptop computers
- Servers including multiple disk storage
- USB devices
- CD/DVDs
- Floppy disks
- Backup devices including tapes

New sources of electronic evidence

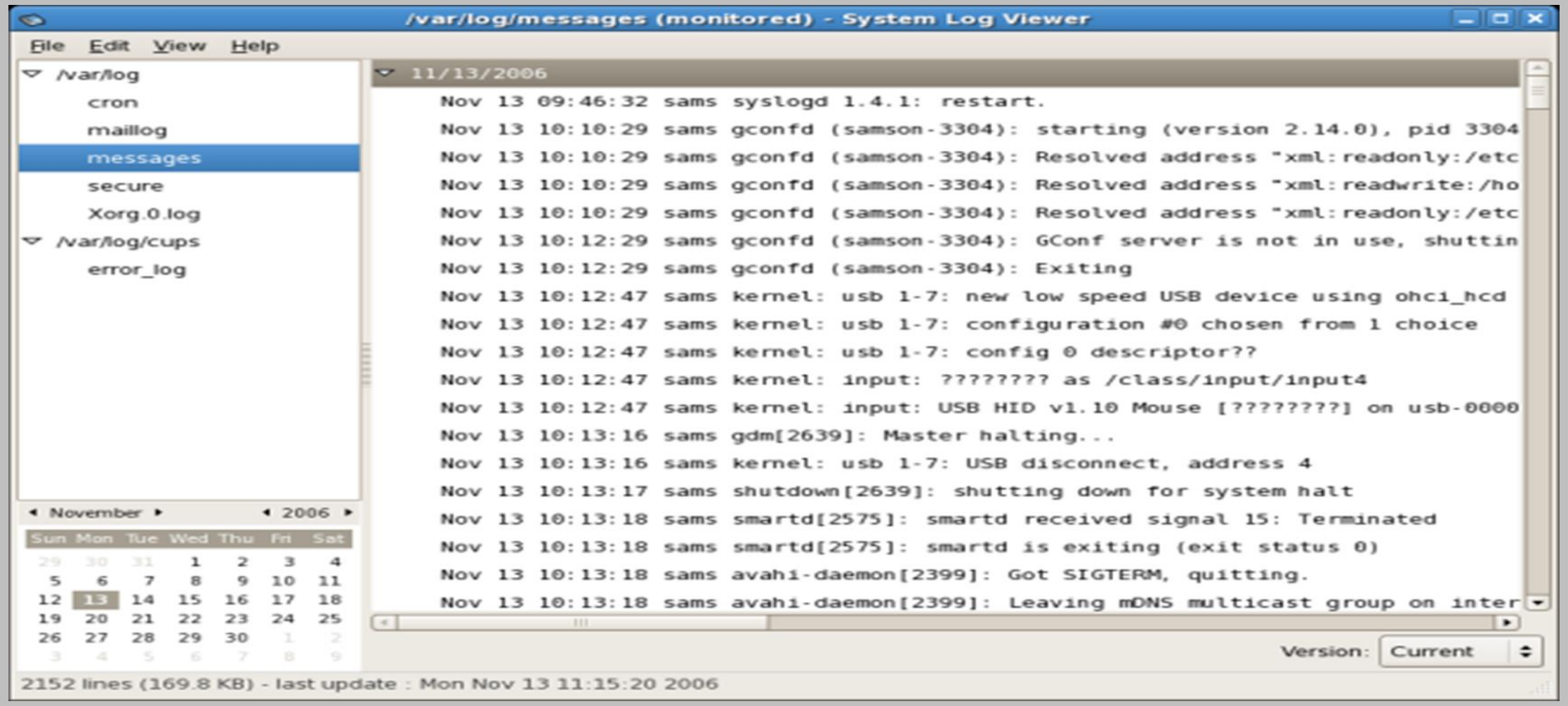
- Mobile phones including smart phones
- GPS navigation devices – these devices can record location data
- Multi-Function Printers (MFP's) – these devices can store print logs and potentially print jobs
- Digital video recorders
- Digital voice recorders
- Digital still cameras including SD/CF cards and other types of memory cards
- Internet and cloud storage (see callout box below)

Types of Evidence available on a computer

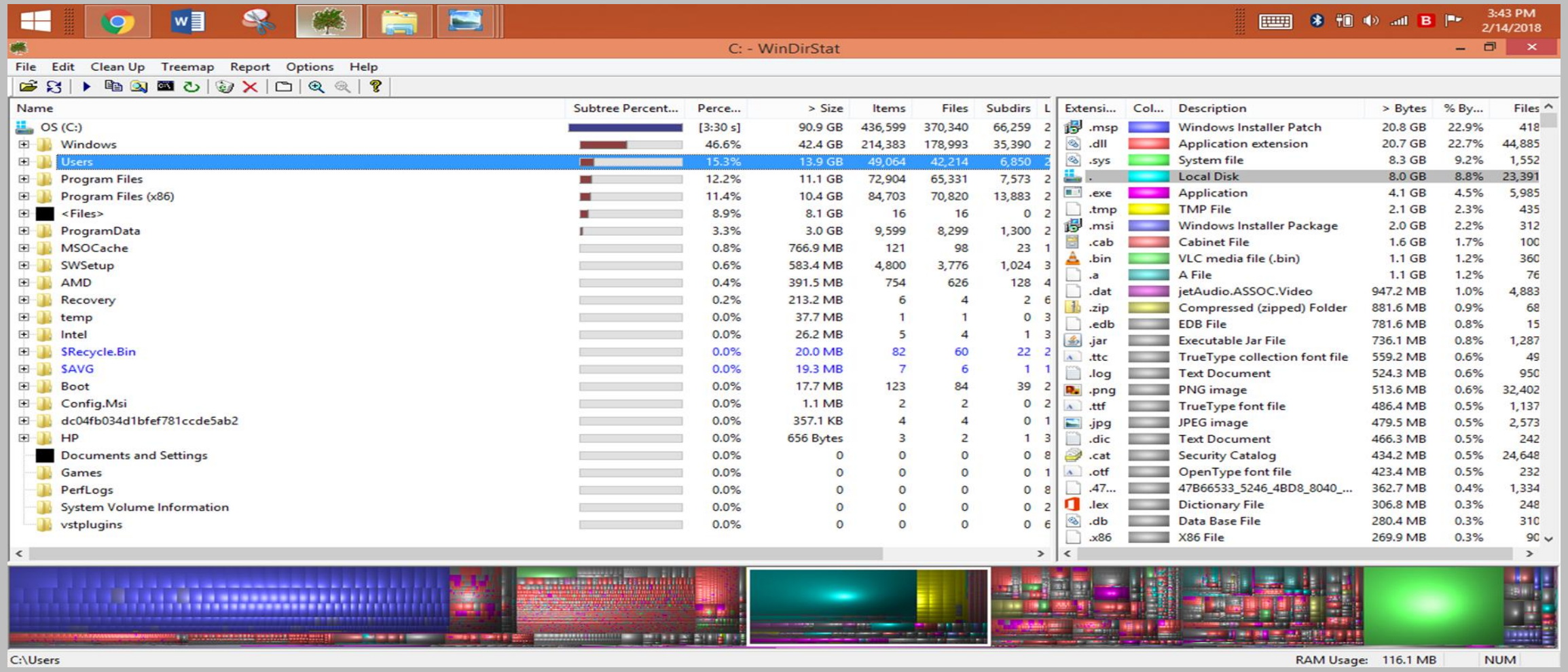
- Files & Logs
- Documents or files created or modified by user
- System & program files
- Temporary & cache files
- Deleted files



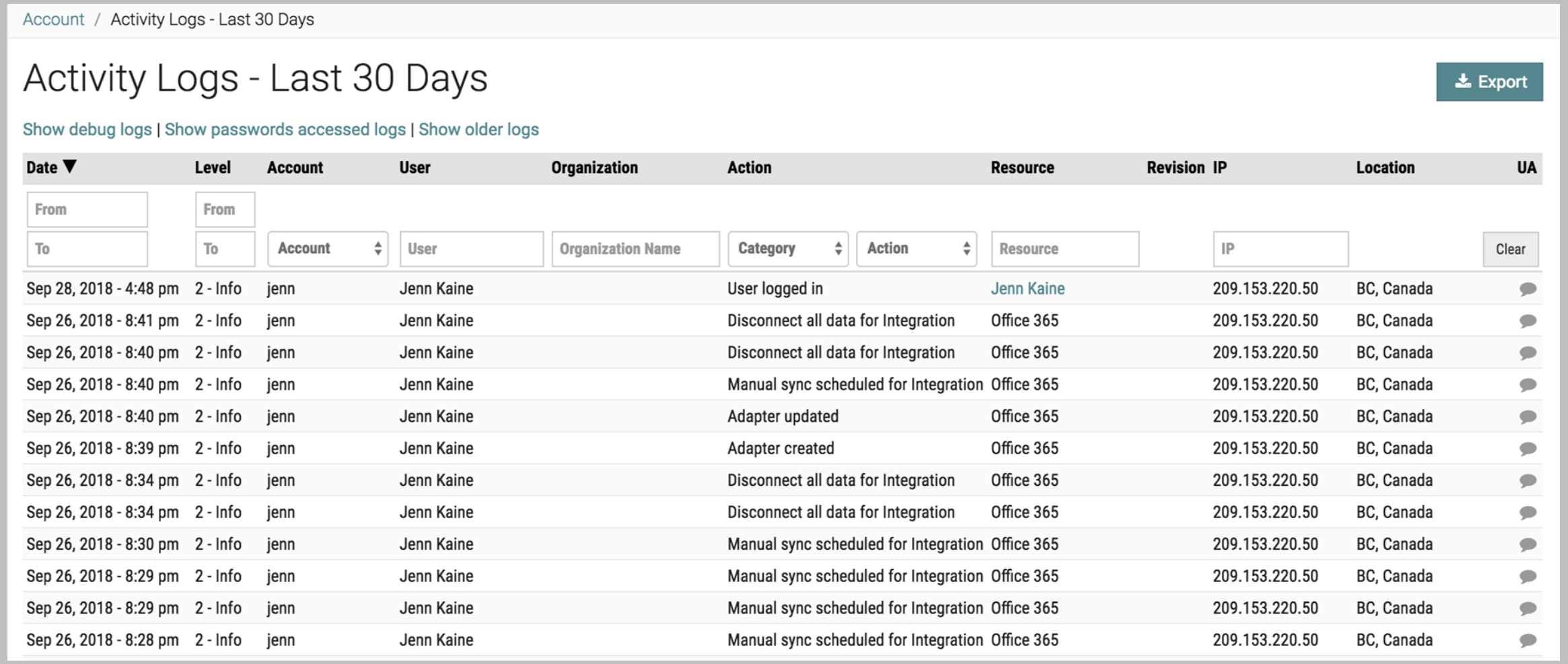
System Logs


/var/log/messages (monitored) - System Log Viewer
File Edit View Help
/var/log
cron
maillog
messages
secure
Xorg.0.log
/var/log/cups
error_log
11/13/2006
Nov 13 09:46:32 sams syslogd 1.4.1: restart.
Nov 13 10:10:29 sams gconfd (samson-3304): starting (version 2.14.0), pid 3304
Nov 13 10:10:29 sams gconfd (samson-3304): Resolved address "xml:readonly:/etc
Nov 13 10:10:29 sams gconfd (samson-3304): Resolved address "xml:readwrite:/ho
Nov 13 10:10:29 sams gconfd (samson-3304): Resolved address "xml:readonly:/etc
Nov 13 10:12:29 sams gconfd (samson-3304): GConf server is not in use, shuttin
Nov 13 10:12:29 sams gconfd (samson-3304): Exiting
Nov 13 10:12:47 sams kernel: usb 1-7: new low speed USB device using ohci_hcd
Nov 13 10:12:47 sams kernel: usb 1-7: configuration #0 chosen from 1 choice
Nov 13 10:12:47 sams kernel: usb 1-7: config 0 descriptor??
Nov 13 10:12:47 sams kernel: input: ???????? as /class/input/input4
Nov 13 10:12:47 sams kernel: input: USB HID v1.10 Mouse [????????] on usb-0000
Nov 13 10:13:16 sams gdm[2639]: Master halting...
Nov 13 10:13:16 sams kernel: usb 1-7: USB disconnect, address 4
Nov 13 10:13:17 sams shutdown[2639]: shutting down for system halt
Nov 13 10:13:18 sams smartd[2575]: smartd received signal 15: Terminated
Nov 13 10:13:18 sams smartd[2575]: smartd is exiting (exit status 0)
Nov 13 10:13:18 sams avahi-daemon[2399]: Got SIGTERM, quitting.
Nov 13 10:13:18 sams avahi-daemon[2399]: Leaving mDNS multicast group on inter
November
2006
Sun Mon Tue Wed Thu Fri Sat
Version: Current
2152 lines (169.8 KB) - last update : Mon Nov 13 11:15:20 2006

Program Files



Activity Logs



Account / Activity Logs - Last 30 Days

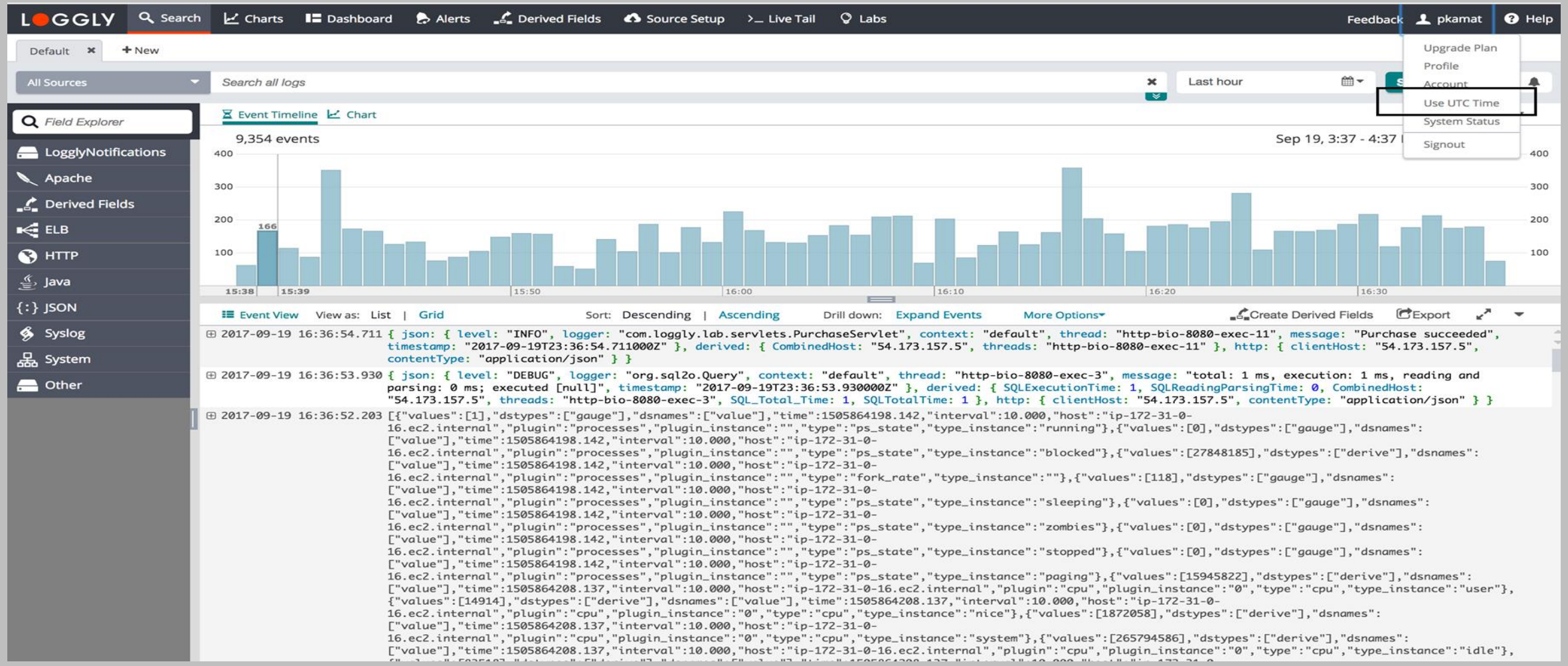
Activity Logs - Last 30 Days

Export

Show debug logs | Show passwords accessed logs | Show older logs

Date ▼	Level	Account	User	Organization	Action	Resource	Revision	IP	Location	UA
From / To	From / To	Account	User	Organization Name	Category / Action	Resource		IP		Clear
Sep 28, 2018 - 4:48 pm	2 - Info	jenn	Jenn Kaine		User logged in	Jenn Kaine		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:41 pm	2 - Info	jenn	Jenn Kaine		Disconnect all data for Integration	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:40 pm	2 - Info	jenn	Jenn Kaine		Disconnect all data for Integration	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:40 pm	2 - Info	jenn	Jenn Kaine		Manual sync scheduled for Integration	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:40 pm	2 - Info	jenn	Jenn Kaine		Adapter updated	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:39 pm	2 - Info	jenn	Jenn Kaine		Adapter created	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:34 pm	2 - Info	jenn	Jenn Kaine		Disconnect all data for Integration	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:34 pm	2 - Info	jenn	Jenn Kaine		Disconnect all data for Integration	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:30 pm	2 - Info	jenn	Jenn Kaine		Manual sync scheduled for Integration	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:29 pm	2 - Info	jenn	Jenn Kaine		Manual sync scheduled for Integration	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:29 pm	2 - Info	jenn	Jenn Kaine		Manual sync scheduled for Integration	Office 365		209.153.220.50	BC, Canada	
Sep 26, 2018 - 8:28 pm	2 - Info	jenn	Jenn Kaine		Manual sync scheduled for Integration	Office 365		209.153.220.50	BC, Canada	

Time Stamps


LOGGLY
Search
Charts
Dashboard
Alerts
Derived Fields
Source Setup
Live Tail
Labs
Feedback
pkamat
Help
Default
+ New
Upgrade Plan
Profile
Account
Use UTC Time
System Status
Signout
All Sources
Search all logs
Last hour
Field Explorer
LogglyNotifications
Apache
Derived Fields
ELB
HTTP
Java
JSON
Syslog
System
Other
Event Timeline
Chart
9,354 events
Sep 19, 3:37 - 4:37
400
300
200
100
166
15:38
15:39
15:50
16:00
16:10
16:20
16:30
Event View
View as: List | Grid
Sort: Descending | Ascending
Drill down: Expand Events
More Options
Create Derived Fields
Export
2017-09-19 16:36:54.711 { json: { level: "INFO", logger: "com.loggly.lab.servlets.PurchaseServlet", context: "default", thread: "http-bio-8080-exec-11", message: "Purchase succeeded", timestamp: "2017-09-19T23:36:54.711000Z" }, derived: { CombinedHost: "54.173.157.5", threads: "http-bio-8080-exec-11" }, http: { clientHost: "54.173.157.5", contentType: "application/json" } }
2017-09-19 16:36:53.930 { json: { level: "DEBUG", logger: "org.sql2o.Query", context: "default", thread: "http-bio-8080-exec-3", message: "total: 1 ms, execution: 1 ms, reading and parsing: 0 ms; executed [null]", timestamp: "2017-09-19T23:36:53.930000Z" }, derived: { SQLExecutionTime: 1, SQLReadingParsingTime: 0, CombinedHost: "54.173.157.5", threads: "http-bio-8080-exec-3", SQL_Total_Time: 1, SQLTotalTime: 1 }, http: { clientHost: "54.173.157.5", contentType: "application/json" } }
2017-09-19 16:36:52.203 [{"values":[1],"dstypes":["gauge"],"dsnames":["value"],"time":1505864198.142,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"processes","plugin_instance":"","type":"ps_state","type_instance":"running"},{"values":[0],"dstypes":["gauge"],"dsnames":["value"],"time":1505864198.142,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"processes","plugin_instance":"","type":"ps_state","type_instance":"blocked"},{"values":[27848185],"dstypes":["derive"],"dsnames":["value"],"time":1505864198.142,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"processes","plugin_instance":"","type":"fork_rate","type_instance":""},{"values":[118],"dstypes":["gauge"],"dsnames":["value"],"time":1505864198.142,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"processes","plugin_instance":"","type":"ps_state","type_instance":"sleeping"},{"values":[0],"dstypes":["gauge"],"dsnames":["value"],"time":1505864198.142,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"processes","plugin_instance":"","type":"ps_state","type_instance":"zombies"},{"values":[0],"dstypes":["gauge"],"dsnames":["value"],"time":1505864198.142,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"processes","plugin_instance":"","type":"ps_state","type_instance":"stopped"},{"values":[0],"dstypes":["gauge"],"dsnames":["value"],"time":1505864198.142,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"processes","plugin_instance":"","type":"ps_state","type_instance":"paging"},{"values":[15945822],"dstypes":["derive"],"dsnames":["value"],"time":1505864208.137,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"cpu","plugin_instance":"0","type":"cpu","type_instance":"user"},{"values":[14914],"dstypes":["derive"],"dsnames":["value"],"time":1505864208.137,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"cpu","plugin_instance":"0","type":"cpu","type_instance":"nice"},{"values":[1872058],"dstypes":["derive"],"dsnames":["value"],"time":1505864208.137,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"cpu","plugin_instance":"0","type":"cpu","type_instance":"system"},{"values":[265794586],"dstypes":["derive"],"dsnames":["value"],"time":1505864208.137,"interval":10.000,"host":"ip-172-31-0-16.ec2.internal","plugin":"cpu","plugin_instance":"0","type":"cpu","type_instance":"idle"},

Meta Data


Data
Metadata
Filename:
Tadzik.jpg
Author:
Piotr Kononow
Date:
August 15, 2016

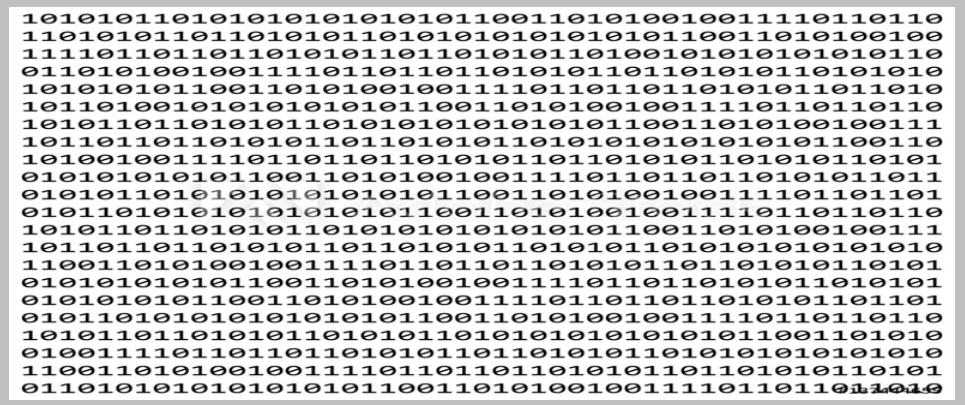
Admissibility of Electronic Evidence

- Parliament in its wisdom Incorporated Ss. 65A & 65B in the Evidence Act.
- S. 65A is termed as-special provisions as to evidence relating to electronic record. Ss. 65A & 65B are a complete code in a code.
- ***S.65B. Admissibility of electronic record-*** requires special procedure for presenting electronic records as admissible in evidence, in a Court of law. It provides for technical and non-technical conditions and the method for presenting electronic records as admissible in evidence

MYTH OF PRIMARY & SECONDARY EVIDENCE

- Primary evidence means **the document itself.**

- PRIMARY format of what gets written as electronic record , **is computer-readable but is not human- readable**.

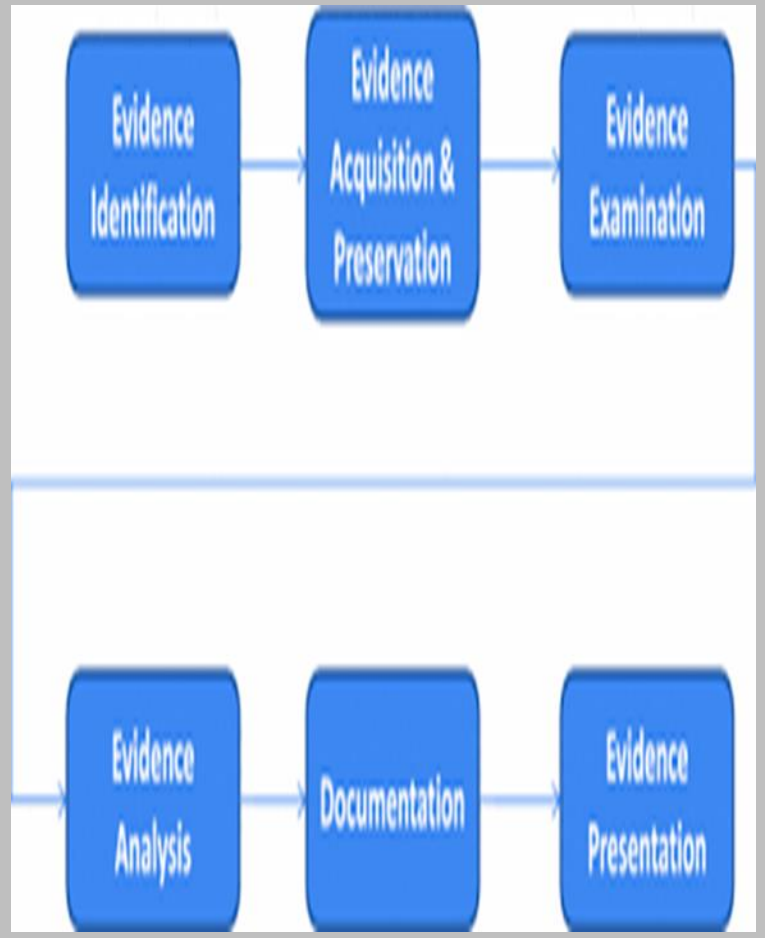


Hence, there can be little or rather, no distinction between primary evidence and secondary evidence in relation to digital/electronic records.

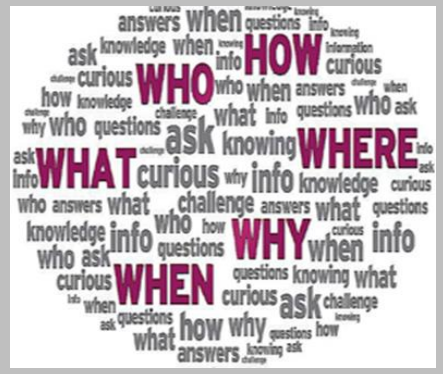
With this understanding, it could **ONLY** be secondary evidence that could be produced in the court with regard to electronic records.

Collection & chain of custody of digital evidence

WHAT IS CHAIN OF CUSTODY & EVIDENCE HANDLING?



As electronic evidence is easy to tamper or to get damaged, it is necessary for the court to know exactly who, what, when, where, and why was the evidence transferred to the concerned person.
It will not be possible to prove the integrity of the evidence, if the chain of custody is not properly maintained.

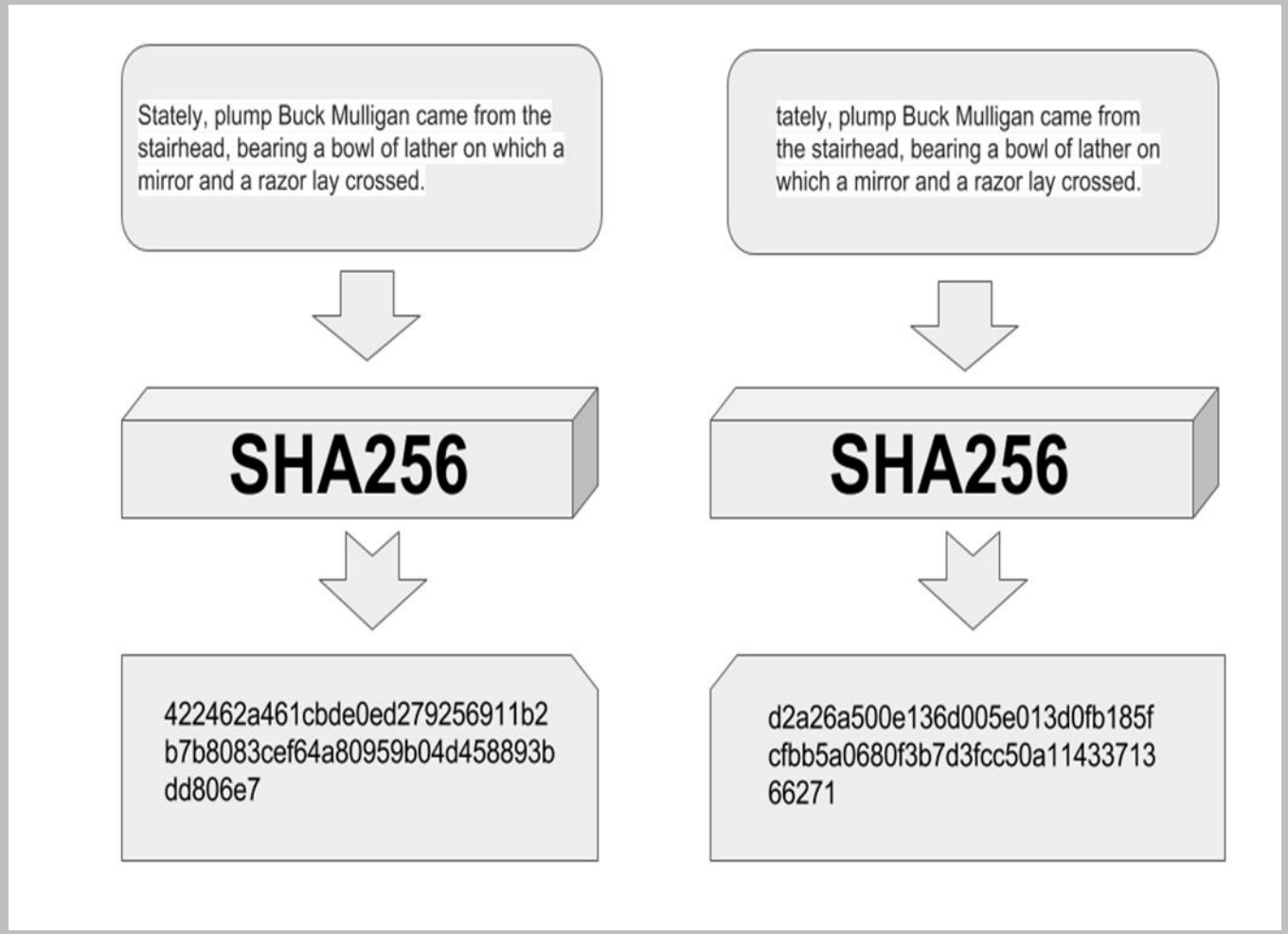


- Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence.
- These would be -

1. People who have seized the equipment
2. People who are in charge of transferring the evidence from the crime scene to the forensic labs.
3. People in charge of analysing the evidence, and so on.

Important Points to remember for Fool-proof Chain of Custody

- Always accompany evidence with their **chain-of-custody forms**
- Give the evidence **positive identification** at all times that is legible and written with permanent ink.
- Establishing the **integrity** of the seized evidence through forensically proven procedure -"Hashing"
- Hashing helps the IO to prove the integrity of the evidence. Similarly, the seized original evidence can be continued to be checked for its integrity by comparing its hash value, to identify any changes to it.



Some key elements that require documentation

- **How** the evidence was **collected**
- **When** was it **collected** (e.g. Date, Time)
- **How** was it **transported**
- **How** was it **tracked**
- **How** was it **stored** (for example, in secure storage at your facility)
- **Who has access to the evidence**

Final Thoughts

- Indian Judiciary, though has come a long way in recognizing, accepting, appreciating and assimilating these aspects of digital evidence, its importance and complexity, but there still remains a lot of challenges in the area as technology keeps changing at a fast pace throwing up new challenges and the law has a rather slower pace in keeping abreast .


QUESTIONS
poll
asking
reply
q&a
query
ask
answers
questions
confusion
investigation
interrogation
challenge
problem
puzzle