

9<

VERIFIED SEARCH WARRANT

SYSTEMS

SUSPECT DETAILS

DESKTOPS

IDENTIFICATION PHASE

LAPTOPS

EVIDENCE ITEMS

SUSPECT DETAILS

PROCEDURES

ENTERTAINMENT DEVICES

SMART TVS

SMART WATCHES

TABLETS

SMART PHONES

OTHER EVIDENCE

CHAIN OF CUSTODY DOCUMENTS

IDENTIFICATION

HAS POTENTIAL	CONSISTS OF
REQUIRE	MAY CONTAIN
ARE	CONTAINS
MAY HAVE	MAY HAVE
HAS POTENTIAL	HAS POTENTIAL
HAS	HAS
MAY HAVE	MAY HAVE
HAS POTENTIAL	HAS POTENTIAL
HAS	HAS



CHAIN OF CUSTODY INCIDENT REPORT INFORMATION FORMS ARCHIVE TAG PROCEDURES REGULATIONS LEGLISLATION LOG **LOG INFO DOCUMENTATION**

PRESERVATION

Tanner, A. and Dampier, D., 2009, January. Concept mapping for digital forensic investigations. In IFIP International Conference on Digital Forensics (pp. 291-300). Springer, Berlin, Heidelberg.

S

HAS POTENTIAL	CONSISTS OF
REQUIRE	MAY CONTAIN
CONTAINS	
HAS SPECIFIC	
CONSISTS OF	
PERTAINS TO	
MUST KEEP RECORDS OF	



8<

APPROVED HARDWARE

IMAGING TOOLS

APPROVED SOFTWARE

IMAGING SOFTWARE

DATA RECOVERY SOFTWARE

FTK IMAGER

FORENSIC TOOLKIT

DD

USDOJ

IMAGE MASSTER SOLO 3

APPROVED METHODS

AUTHENTICATION

COLLECTION PHASE CONCEPT

ENCASE

DOCUMENTATION

ELATIONS

COLLECTION

MUST HAVE	CAN BE
USES	SUCH AS
USES	
USES	
CONSISTS OF	
AVAILABLE AS	
THAT IS ACCEPTABLE FOR USE	
AVAILABLE AS	
CAN BE USED FOR EVIDENCE	



9<

APPROVED METHODS

IMAGES

APPROVED SOFTWARE

FILES

ENCASE

SWAP SPACE

FORENSIC TOOLKIT

SLACK SPACE

USDOJ

FOLDERS

METHODS USED IN ORGANISATION

EVIDENCE CASE REPORT

OTHER AREAS

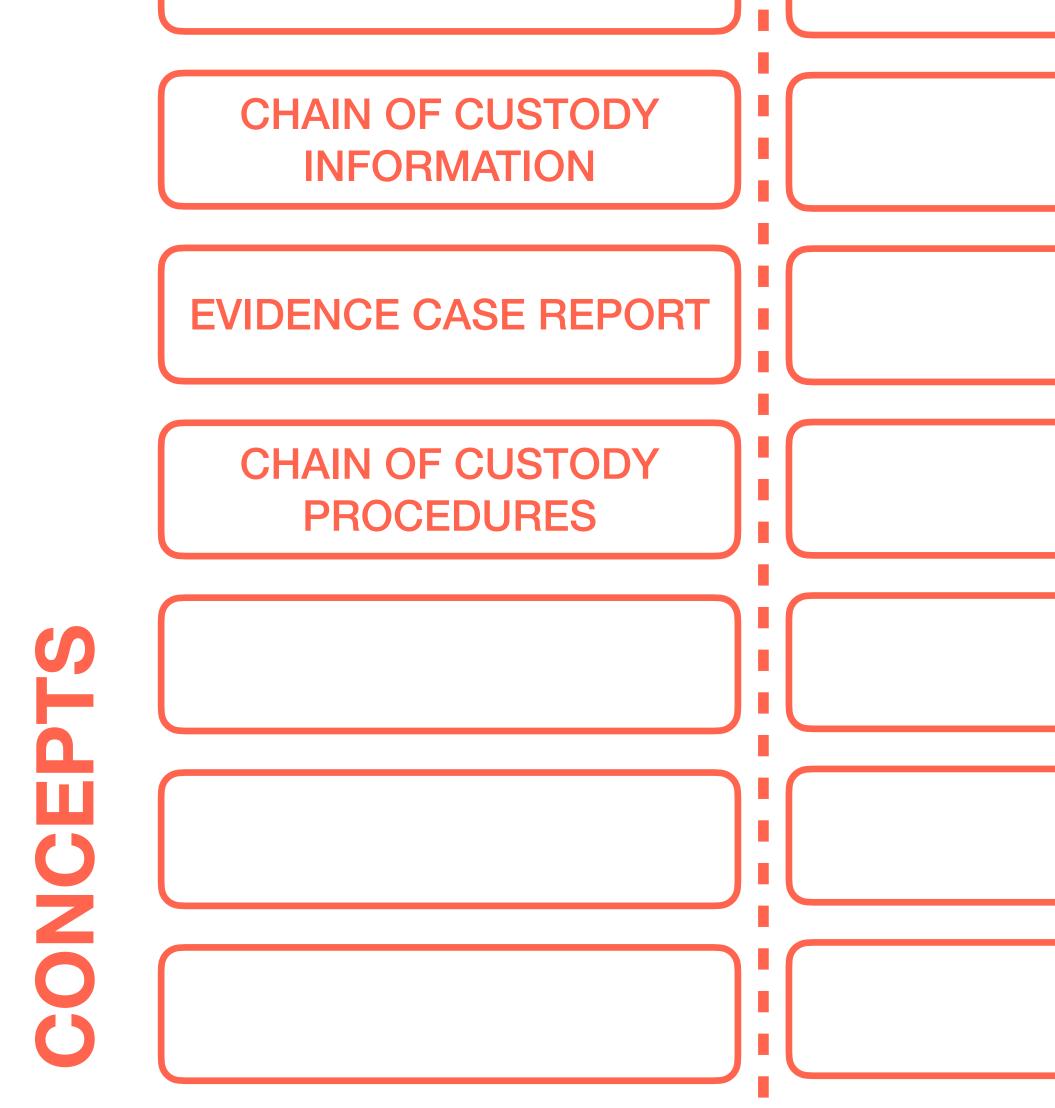
EVIDENCE BOOKMARKS

REGISTRY

DELETED ITEMS

EXAMINATION

CONTAINS	CAN BE
USES	SUCH AS
RECORDED IN	RESULTS IN
RECORDED IN	
AND THOSE	
BASED ON	
THAT CAN BE USED	
RECORDED IN	
RECORDED IN	



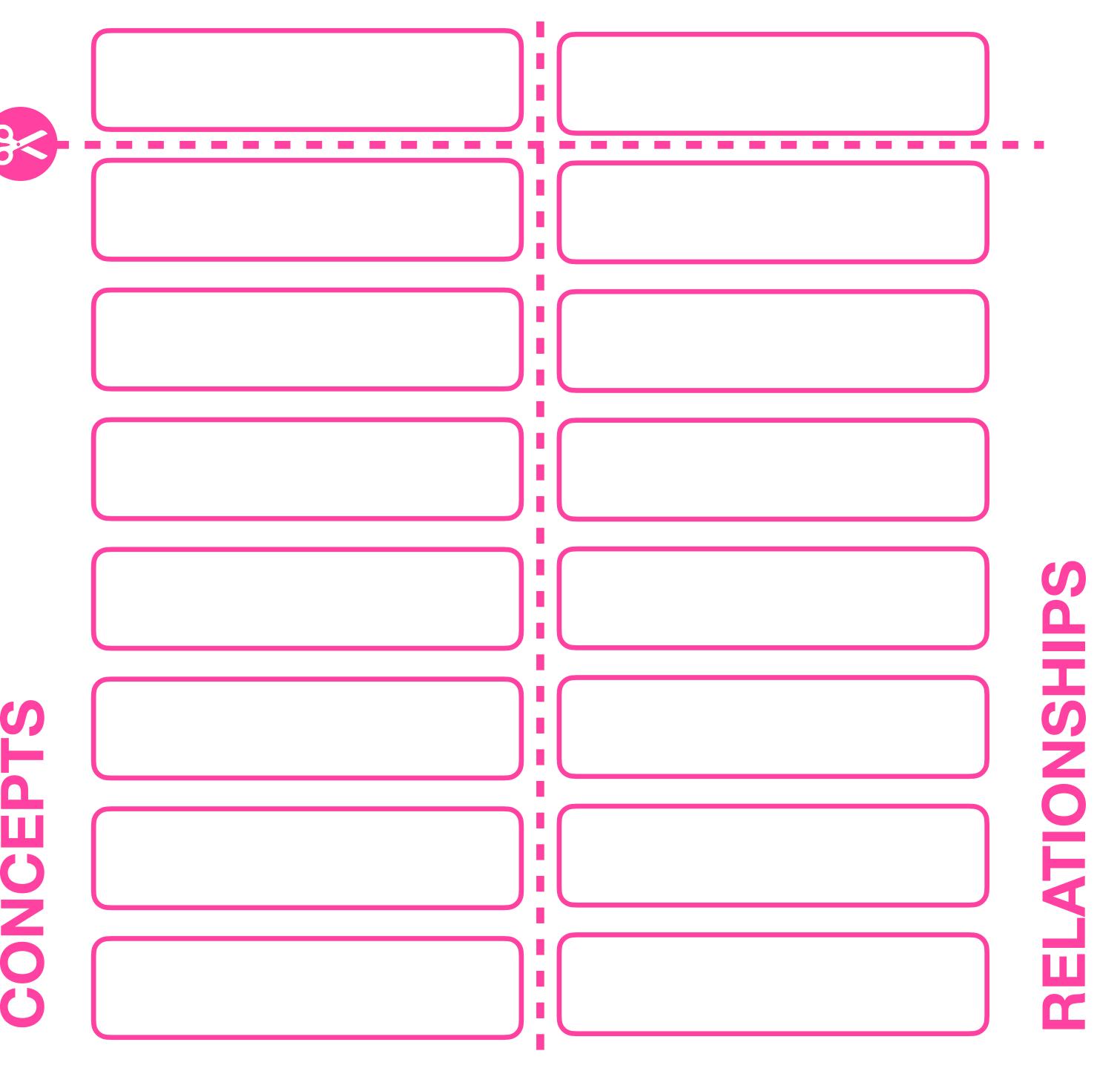
VERIFIED SEARCH

WARRANT

SUSPECT DETAILS

CONTAINS	CAN BE
USES	SUCH AS
RECORDED IN	RESULTS IN
CAN BE USED IN	
INFO USEFUL TO	
CONTAINS	
FINDINGS CAN BE USED IN	
MAY BE USEFUL TO	
HAS	

ANALYSIS



PRESENTATION