XCompany Chain of Custody Form

By company policy, all seizures and investigations of incident procedure require the use of this form. The purpose of this form is to track evidence and possession of such during investigation. Doing so will preserve the integrity of the evidence and prevent it from contamination, which can alter the state of the evidence. If not preserved, the evidence presented in court might be challenged and ruled inadmissible. All curators of evidence are required to record asset details and show proof of validation for the information entered.

Case #:	**Date of Event:**

Description of Evidence

Item #	Evidence Type/ Manufacturer	Serial #	Item Owner/Title	Description

Chain of Custody

Date/Time	Item #	From	To	Reason
Date:		Name/Organization:	Name/Organization:	
Time:		Signature:	Signature:	
Date:		Name/Organization:	Name/Organization:	
Time:		Signature:	Signature:	
Date:		Name/Organization:	Name/Organization:	
Time:		Signature:	Signature:	
Date:		Name/Organization:	Name/Organization:	
Time:		Signature:	Signature:	
Date:		Name/Organization:	Name/Organization:	
Time		Signature:	Signature:	

All parties are required to sign

XCompany MacOS Memory Imaging Checklist

Step:	To Do:	Signature:	Date/ Time:
Step 1 – Prepare Acquisition Media	Download MacPmem and unzip to acquisition drive. https://github.com/google/rekall/releases/download/v1.5.1/osxpmem-2.1.post4.zip Note: Ownership needs to be root:wheel *$Sudo chown root:wheel MacPmem.kex* Have External drive ready for use		
Step2 – Load MacPmem Kernel Driver	OSXPmem uses a kernel driver to capture the memory. Load it with kextload. *$sudo kextload MacPmem.kext*		
Step 3- Create Image	With the kernel driver loaded the memory image can now be created. *$Sudo ./osxpmem –output case_image.aff4*		
Step 4- Unload Kernel Driver	With the memory image created the kernel driver can be unloaded. *$Sudo kextunload MacPmem.kext*		
Step 5 – Collect Profile Information	After you have created the disk image it is good practice to collect information about the Mac the image was created on. The following two commands will do that. *$sw_vers > osxbuildinfo.txt*		

-All Steps must be documented and followed. If there are any concerns, please inquire the lead of the investigation for further questions.