AFRL Digital Forensic Research Workshop

DFRWS 2004 Workshop Report and Findings

Chester J. Maciag, Editor
AFRL Information Directorate

Sponsored by:
Air Force Research Laboratory Information Directorate
AFRL/IFGB, 525 Brooks Rd., Rome NY 13441-4505

Executive Summary

The fourth annual Digital Forensics Research Workshop was held August 11-13 2004 in Baltimore MD. DFRWS 2004 was sponsored by the Air Force Research Lab Information Directorate, and held in conjunction with the NIST Hashapalooza conference. Over 110 law enforcement practitioners, academics, scientists, industry experts, and DoD representatives participated. Each day of DFRWS adhered to a main theme, and consisted of a keynote, paper presentations, panel discussions, workshops, and briefs back to the plenary group. There was fun to be had as well, through the traditional evening activities of Forensic Feud, Forensic Rodeo, and the DFRWS Dinner.

The theme for Day 1 was to advance the digital forensic investigative framework outlined in the first workshop report (2001). Mark Pollitt, formerly of the FBI, served as keynote, followed by papers from Nicole Beebe, Florance Tushabe, and Brian Carrier. The panel discussion was comprised of James Cristy, Chet Hosmer, and Chris Sanft. Workshops were led by Dario Forte, James Lyle, Eoghan Casey, Gary Palmer, and Mark Pollitt. The main outcome of Day 1 was the realization that no single framework will suffice to meet the needs of all practitioners, forensic investigators, and computer network defense professionals. Instead, general processes will need to be adapted to provide the specific detailed steps, procedures, or iterations that are appropriate for the domain of application.

Addressing the technical and procedural barriers to “In-Time” forensic investigation was the theme for Day 2. Lance Spitzner of the Honeynet Project provided the keynote address, followed by papers from Edward Balas, Heather Dussault, John Lowry, and Golden Richard. The panel discussion was comprised of Phil Turner, James Collins, Frank Adelstein, and John Ward. Workshops were led by Golden Richard, Chet Maciag, Jack Mineo, Heather Dussault, and Chet Hosmer.

Day 3 was composed of papers accepted to the DFRWS that did not fall clearly into the two predominant themes, yet were deemed to have

important value in generating scientific discussion or sharing technical information. Ian Bryant, Mark Hirsh, and Mike Seiffert presented papers, while Hashapolooza took place concurrently in another room. Following the presentation of papers, the DFRWS community convened to discuss the overall impressions of the workshop, and provided input on topics that should be addressed in 2005.

Table of Contents

List of Figures

List of Tables

Acknowledgements

This technical report is the culmination of the hard work of many individuals that collectively supported DFRWS 2004. The editor acknowledges the following individuals and their dedicated efforts:

- Nicole Beebe, Kyle Dempsey, Eric Ozanam, Thomas Parisi, Scott Rey, Mark Williams, and Laura Wood, for carefully recording individual workshop session discussions;

- Tanya Allen and Nelson Lee, who, in addition to serving as recorders, also helped arrange and format all notes for the editor prior to writing;

- Dan Kalil, for making our workshop's local arrangements and ensuring that all logistical concerns were addressed, allowing attendees to focus on the tasking at hand;

- Gary Palmer, for serving once again as technical chair, and helping to engage the forensic community to participate in the workshop;

- Eoghan Casey, Chet Hosmer, Heather Dussault, James Lyle, Jack Mineo, Mark Pollitt, Golden Richard III, Dario Forte, and other facilitators who help bring order to the sometimes chaotic discussions of the workshops, and;

- The DFRWS forensic research community, for their hard work during the workshop in advancing the understanding of the role of frameworks for digital investigation. Also, for developing scientific approaches for achieving in-time analysis capabilities. DFRWS thanks you for your continued support.

Finally, the editor would like to acknowledge the continued support provided to DFRWS by the Air Force Research Laboratory, Information Directorate, without which, DFRWS 2001-2004 would not have been possible.

DFRWS Background

The Digital Forensic Research Workshop (DFRWS) was conceived in August 2001 under the sponsorship of the Air Force Research Laboratory (AFRL) Information Directorate, Rome Research Site. The purpose of DFRWS was to:

- Initiate a dynamic community of experts from academia and practice
- Promote scholarly discussion related to digital forensic research and its application
- Involve experienced analysts and examiners from LE, military and civilian sectors
- Define core technologies that form the focus of useful research
- Establish a common lexicon so the community speaks the same language
- Engage in regular collaborative activity to keep focus sharp and interest high

Each year since, the DFRWS community has grown, from a mere 50 attendees in 2001 to over 120 in 2004, and representing eight countries. Attendees come from Academia, Industry, Law Enforcement, Legal, Federal Government, and the Department of Defense, and include scientists, tool builders, tool users, and legal advisors. Topics have included Framework, Standards and Methods, Current Challenges, Digital Forensic Research, and In-Time Forensic Analysis.

DFRWS has been long supported and sustained by its members – you. DFRWS 2005 marks a transition for the workshop, as it transitions to a self-governing, not-for-profit organization independent of Air Force support.

Day 1 – Framework

Introduction (From the Call for Papers)

This field or discipline we are calling Digital Forensics ultimately exists to aid in the identification and possibly the prevention of wrongdoing by discovering and clearly presenting evidence obtained from digital sources. Directly or indirectly, investigators employing methods, technologies, and tools in this new discipline follow some prescribed set of steps or procedures. The path can stem from merely being informed of a possible event as a crime or an anomaly, through processing data and exhibits toward some sort of decision or outcome in courts or law or in command decision-making in a commercial, military or CIP (Critical Infrastructure Protection) operational environment. As the investigation progresses, examiners and analysts employ an assortment of protocols and technologies to assist. As of today, there is no clear, agreed upon categorization for these mappings. Having this would allow specialization or technological concentrations so that continuous, focused discovery and enhancement would occur.

Since the initial workshop, DFRWS 2001, an outline (contained in the Roadmap Document) of one potential approach to defining a set of categories has been proposed. Since then, there has been a significant debate about the operational features and limitations of this investigative framework. Consideration of multiple perspectives will start the formation of a more applicable set of connected steps in a Digital Forensic Framework. Each step will be clearly defined and associated with existing technologies and tool sets that may have forensic applications. As a by-product, the “matrix” that will be produced will also pinpoint shortfalls and limitations in capabilities and technologies addressing certain stages. This will help to set and focus a yearly research agenda toward addressing those areas.

Digital Forensics needs a descriptive framework that describes major fundamental investigative areas and the technologies and processes associated with each. Today we will begin to build a “workable”

Framework for Digital Forensics, adopted through consensus by academics, professionals, and enthusiasts involved in our community. The results of our efforts at DFRWS will be made available to the widest audience possible for review, debate and involvement. We realize we need the widest possible consensus

To attain this goal, several alternate approaches to designing framework were presented, followed by a brief panel discussion and structured breakout sessions involving all attendees. The groups for each breakout session were predetermined to encourage diversity in discussions.

Keynote Presentation

Mark Pollitt, "Six Blind Men From Indostan"

Mr. Pollitt first recounted a tale in which six blind men first encounter an elephant. Each blind man came into contact with a different part of the elephant (e.g. tusk, ear, trunk, leg, torso, and tail). Each blind man had vastly different impressions of the rest of the animal, given the sampling they received. One thought an elephant was like a spear, another like a leaf, another like a rope, etc.) The point of the story is that each blind man's experience governed his perception of the elephant.

What does this have to do with Digital Forensics? We all approach digital forensics from different perspectives and with different goals. Depending on who you are, you might believe that digital forensics is:

- An investigative task
- A forensic science
- A sensor input for computer security analysts
- A part of incident response

The truth is that digital forensics is all of these things. However, we cannot seem to agree on the [common] process that we should use to achieve our organizational goals. Most digital forensic processes (investigative, incident response, scientific, etc.) are linear in nature, with a beginning, and sometimes some feedback loops. We seem

to get hung up on this linear property. We probably need to focus on the individual tasks that are common to all processes.

Pollitt then exhibited the DFRWS 2001 framework, which itself defines a linear process with multiple subtasks. He stated that all the functions that an investigator would need to perform are probably in here. We don’t need to throw away the 2001 framework. However, we need to define appropriate subtasks for the particular organizational pursuit.

As an alternative to these linear processes, Pollitt presented the Zachman Enterprise Architecture (Z-EA) Framework for consideration. Used for defining roles, stakeholders, and interactions in IT enterprise architecture, it provides a useful point of reference for analyzing and integrating complex activities. It describes a series of views (e.g. planner, data owner, technologists, vendors, etc) through with all stakeholders view their requirements or role in the enterprise.

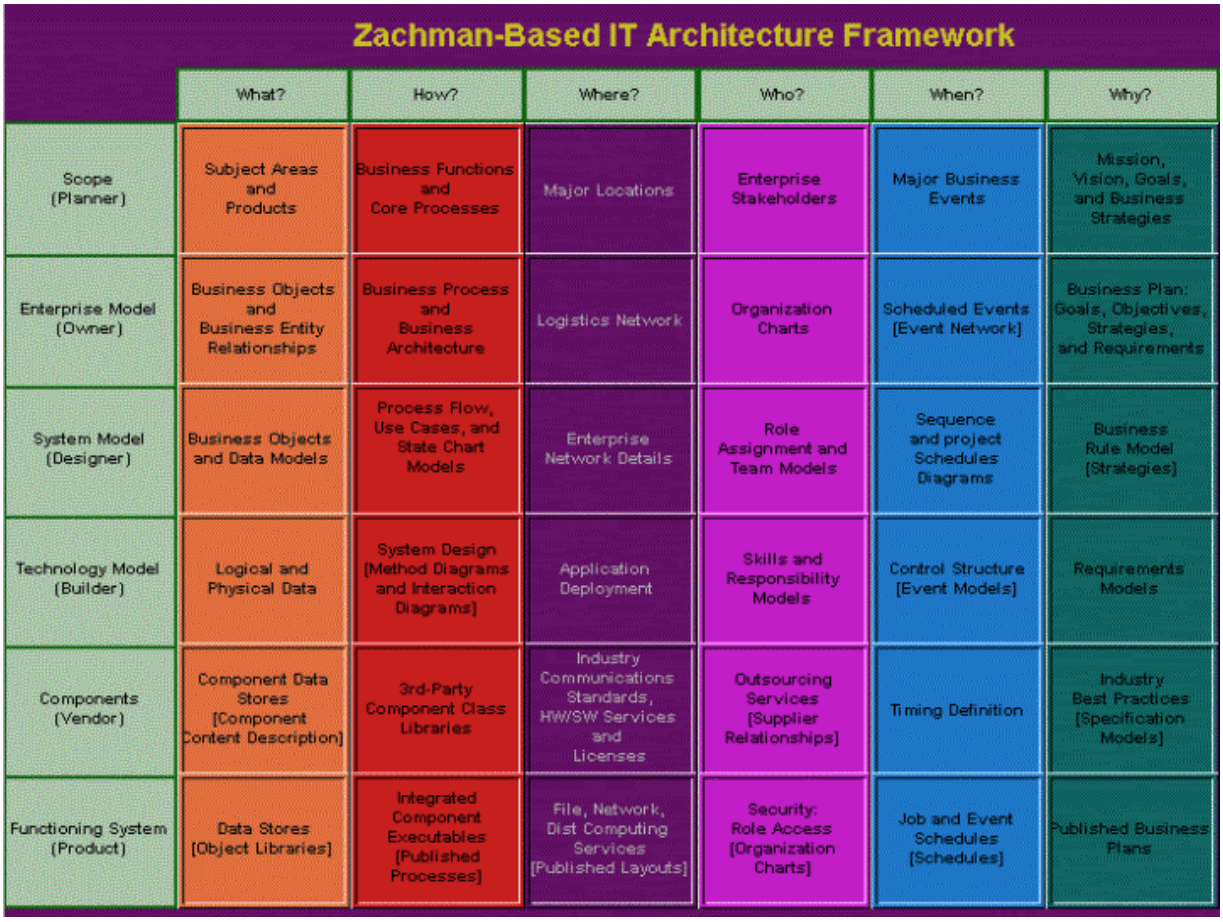

Figure 1 - Zachman Enterprise Architecture Model

We might apply this model to our digital forensics process dilemma. What if the Z-EA Functions (e.g. Who, What, When, How, Why) were replaced with the DFRWS framework of functions – Identification, Preservation, Collection, Examination, Analysis, Presentation? And what if we replaced the Z-EA Views (e.g. Scope, Enterprise Model, etc) with digital forensic roles such as Incident Response, Security Management, Criminal Investigation, etc.? What we would have at the intersections are 'Artifacts', which describe either a function that needs to be performed to accomplish that Function for that particular Role, or a Constraint that needs to be considered in the accomplishment of that Function for that Role. What we have then described is a matrix which captures some unique requirements and constraints for each Role who utilizes the [same] digital forensic framework.

Time, of course, is a sizable source of contention, particularly when discussing the order of forensic functions. Quite often, one's role also defines the order of process and what process steps are utilized. Since_forensics is really about function, we shouldn't get hung up on this. Let's instead just look at the constraints that temporal order imposes. Another way to state this is:

- Forensics is not a single process, but is…
- …a set of tasks that can be grouped into…
- …functions that are selected based upon…
- …the purpose for which the process is being applied (role) and are…
- …bound by constraints that are…
- …defined by either internal or external requirements.

The Z-EA is not the final answer for frameworks. They will continue to evolve in time. You need to decide what works for you. Frameworks have their own values. Test by finding out what works and what doesn't work. Research can be focused on the interrelationship of functions, tasks, constraints, process, and roles.

In summary, the core DFRWS framework is sound. It is suitable to be developed, extended and refined. It can be used as both a framework and a vocabulary.

Questions:

Q1: Can one use the Z-EA to apply [the right] forensic techniques to media?

A1: It is agreed that constraints are VERY important. Apply constraints to examination or you are up creek without paddle. One must look at constraints. I'm not suggesting to change [the entire process], but to evaluate and see if there is a more efficient way of performing media analysis. It would be nice if we could someday model what we do [evaluate it against other potential methods], and come up with the most efficient!

Q2: Would you recommend additional changes for a framework?

A2: I don’t know. No model is perfect in a dynamic environment. But we get better by modeling things. The goal when improving the current frameworks would be to the demands of a dynamic environment.

Plenary Speakers
Several presenters outlined alternatives and enhancements to the framework developed in the 2001 workshop.

Nicole Beebe: "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process"

Editor's Note: This paper has been refined based on discussions at the workshop and was subsequently published in the journal of Digital Investigation.

Ms. Beebe's goal was to develop a flexible, scalable investigative framework that could meet a wide variety of investigative objectives. Beebe's framework approach synthesizes several frameworks, combining the most useful components into a high-level matrix. This matrix can be used to develop application specific matrices. The challenge was to strike a balance between a framework that could support scientifically-rigorous procedures and yet be simple to use and tailor. In application, the framework would be able to be applied to large, complex, criminally relevant investigations, as well as simple, time-critical inquiries. Her work intentionally leveraged existing frameworks and observations from DFRWS, Reith et al, Mandia et al, Carrier and Spafford, and Nelson et al, to arrive at a framework that engenders the diversity of all approaches. All the while, Ms. Beebe's objective was to improve levels of practicality and specificity to meet each investigator's particular needs.

The framework is composed of phases with hierarchical sub-phases. For the most part, phases are general, sequential, and non-iterative stages of the investigation. However, that is not to exclude iteration, for it may be required between phases for particular investigative needs.

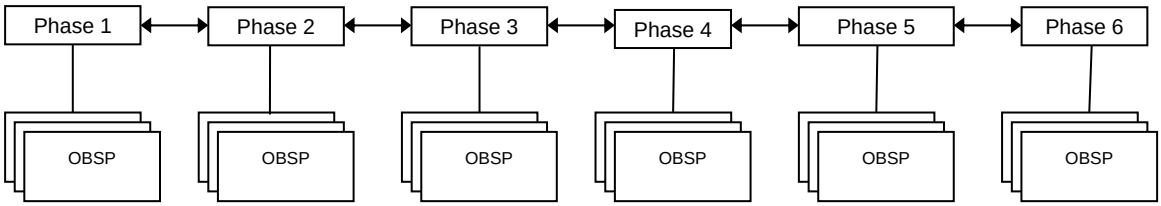

Figure 2 - Hierarchical Phase Structure

Accordingly, each phase has designated sub-phases that define investigative objectives (e.g. “what are you trying to accomplish in this investigative step?”) These objectives are supported by hierarchical, matrixed task structures, and are highly iterative in nature. These object-based sub-phases (OBSP) are intended to vary between specific investigations and types. This framework, in principle, should not preclude continuity of tasks and goals across phases, nor prevent the implementation of investigative standards, guidelines, techniques, and ‘best practices’ already in existence and in use.

In the following Figure, Ms Beebe presented one instantiation of her framework at the highest tier:

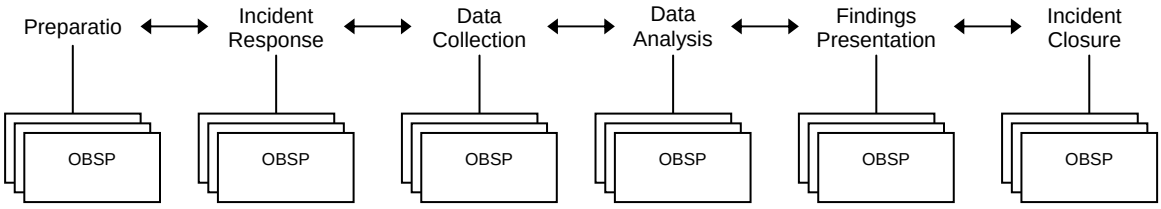

Figure 3 - Proposed Framework, 1st Tier

Note that all phases may not be equally rigorous, nor be spaced equally in an investigative time line. As the 2nd tier is defined, sub-phase objectives need to be articulated. This are is under-addressed, for most investigations define procedures without describing intent. The reverse is true here. If you can define intent, then you might be able to choose from several avenues of obtaining the required information. An example of such an objective might be: “Determine if unauthorized software was installed”, instead of “examine the Registry key…”

An example of iteration within a phase was depicted in the following Figure. Here, the Survey, Extract, and Examine (SEE) data analytical approach has been implemented as an iterative process in order to achieve objectives of "describe digital object's landscape", "extract data for examination", and "examine data to confirm or disprove case theories." Each subphase can have a multitude of tasks that examine high and low-level investigative facets. Similar iterations can tasks can be performed in the 2nd tier of other phases as well, and scaled upon investigative intent and timeframe.

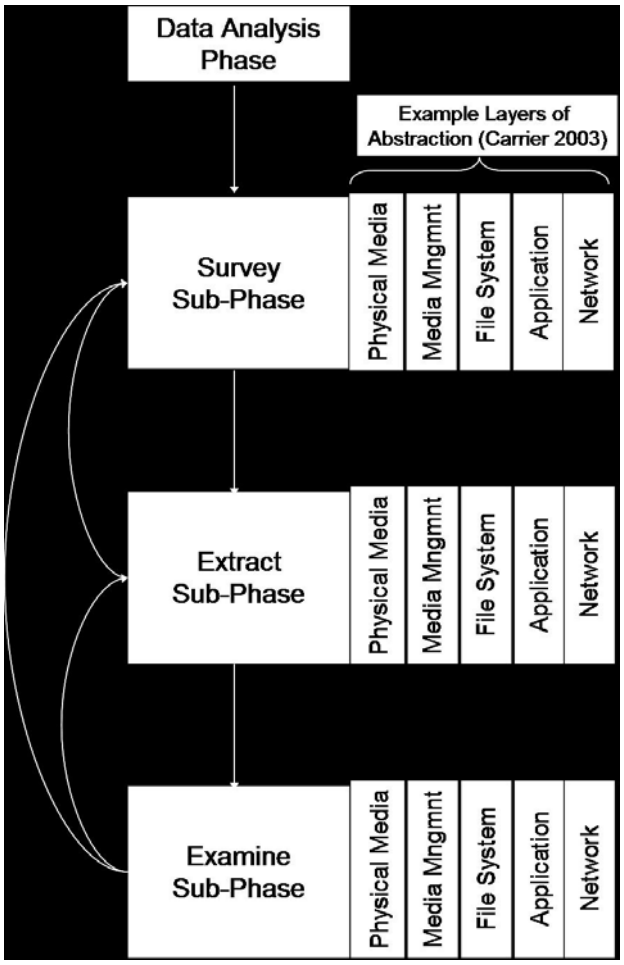

Figure 4 - Interaction Example Within Data Analysis Phase

There are a couple of benefits of this hierarchical, objectives-based approach. One is that it meets criteria spelled out in Carrier and Spafford (2003) in the areas of practicality and specificity that can be used by the entire community. Another benefit is that the approach enables the use of matrices to map between subtasks, tasks, tools, and

objectives. In turn, matrices can help streamline complex, flexible processes, reduce task redundancies, and identify investigative gaps.

Further work will seek to mitigate the framework's primary limitation: it is incomplete, particularly in the area of further refinement of data analytic objectives and task hierarchies. The remaining phases not delved in depth here also need further sub-phase development. A cross-abstraction layer is needed, and finally, empirical testing of the model would be key to gauging the model's utility.

Florence Tushabe: "The Enhanced Digital Investigation Process Model"

Ms. Tushabe's presentation explored and contrasted previously-established forensic investigation process models, noting the similarities and shortcomings between each of them. To address the shortcomings of the current models, Ms. Tushabe proposed a new process model, the Enhanced Digital Investigation Process Model, which was built upon the strengths of the Integrated Digital Forensics Model.

The Forensics Process Model provides a very high-level, four-phased process (Collection, Examination, Analysis, and Reporting) that is to be performed in a forensic investigation. The process is linear and non-recursive (e.g. limits the investigator's ability to revisit the crime scene and gather more evidence.) The DFRWS 2001 Model defined seven linear, more detailed, phases of tasking, to include Identification, Collection, Presentation, and Decision phases. The Abstract Forensics Process Model added yet two more phases (approach and strategy) and replaced the Decision phase with one called Returning Evidence.

Each model is successively more detailed and inclusive. However, none of them are recursive. Furthermore, in IDIP there are few differences between the Approach Strategy and Preparation phases, and they should be combined. Finally, the Preparation phase should be accomplished prior to the Identification phase. These observations served as input to the proposed enhancements to the IDIP Model.

The IDIP Model consists of five phases: Readiness, Deployment, Physical Crime Investigation, Digital Crime Investigation, and Review. Ms. Tushabe noted that IDIP simplifies the forensic process by grouping the phases into an abstract and manageable manner; highlights reconstruction; differentiates between the digital and physical crime scenes; and emphasizes the review of the whole process, while putting the preparation phase before detection of the incident. However, Ms. Tushabe felt there are shortcomings in IDIP because it depicts the deployment phase (Detection and confirmation) as being independent of the digital and physical investigations; it depicts the forensic process as linear; it doesn't draw a clear distinction between investigations at the victim's and suspect's crime scene; and it contains two reconstructions – may sometimes contradict.

The proposed EDIP model also consists of five major phases, which can be navigated recursively as depicted in the following Figure:

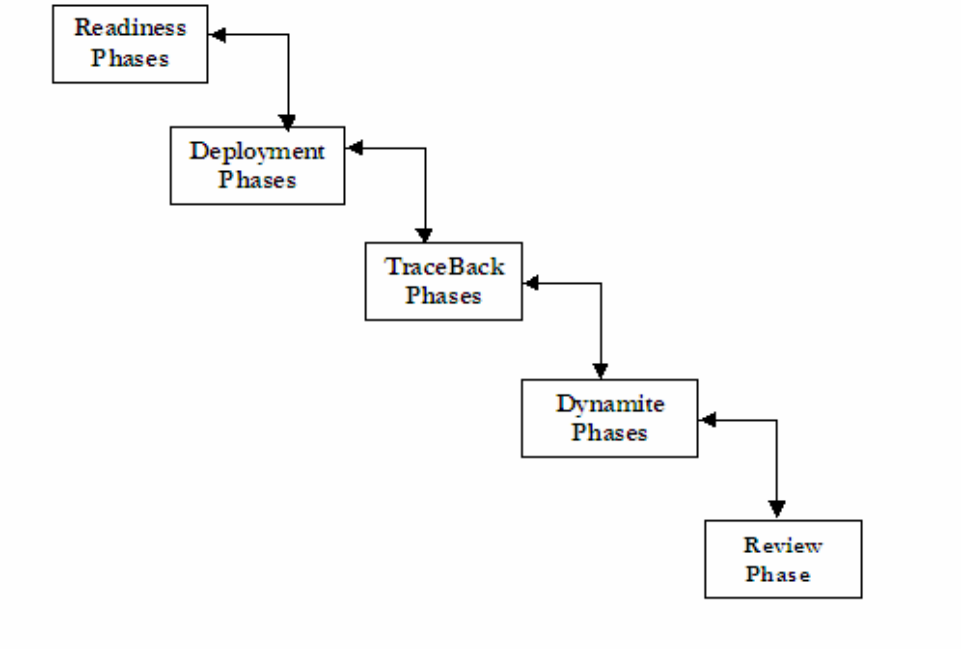

Figure 5 - Phases of the EDIP Model

The IDIP and EDIP share largely similar phases and sub-phases, as depicted in the Table below:

Table 1 - Comparison of Phases Between IDIP and EDIP Models

Phase	**IDIP**	***EDIP***
Review Phases/ *Review Phases*	■Operations ■Infrastructure	■*Operations* ■*Infrastructure*
Deployment phases/ *Deployment phases*	■Detection and notification ■Confirmation and Authorization	■*Detection and notification* ■*Phy crime scene Inv* ■*Dig crime scene inv* ■*Confirmation* ■*Submission*
Physical Crime Scene Investigation phases/ *Traceback phases*	■Presentation ■Survey ■Documentation ■Search and Collection ■Reconstruction ■Presentation	■*Dig crime scene inv* ■*Authorization*
Digital Crime Scene Investigation phases/ *Dynamite Phases*	■Presentation ■Survey ■Documentation ■Search and Collection ■Reconstruction ■Presentation	■*Phy crime scene Inv* ■*Dig crime scene inv* ■*Reconstruction* ■*Communication*
Review phase/*Review*	Review	*Review*

The proposed EDIP Model depicts the forensic process as iterative as opposed to linear. It re-defines the phases in the physical and digital crime scene investigation phases, making them non-exclcusive to a particular investigative phase. Similarly, the Deployment phase is also redefined. The EDIP differentiates the investigation tasking at the primary (suspect) and secondary (victim) crime scenes, and highlights the need for tracing back to the perpetrator's location. Although EDIP reserves only one event reconstruction activity (at the end of the process), it provides for investigative hypotheses (and recursion) during the entire process, making it suitable for cybercrime investigations.

Brian Carrier: "An Event-based Digital Forensic Investigation Framework"

Carrier presented a framework for reconstructing events in a digital crime scene, mapping out the causes and effects of actions (both known and unknown) on objects (both present and missing). Carrier pointed out that there is evidence of an event if remnants of the effect still exist. By preserving the state of a system as close to the time of the events of interest, we are more likely to preserve the effects of those events. However, preservation may not always be necessary depending on the circumstances and goals of the investigation. Provided there is sufficient evidence to enable investigators to reconstruct events reliably, this may be sufficient in some cases (e.g., when investigative leads are needed but evidentiary integrity is not). Few tools facilitate the recreation of events from evidence – this is currently a human process. Carrier presented a model for categorizing objects found at a digital crime scene, reconstructing their relationships, and then their sequence.

Panel Discussion

To initiate debate, a panel discussion was held with three experienced individuals representing R&D in government, private sector, and law enforcement.

Panelists:

- Mr. James Christy, SSA; Director, Defense Cyber Crime Institute, Defense Cyber Crime Center (DC3)
- Mr. Chet Hosmer, Founder and President, Wetstone Technologies, Inc.
- Mr. Chris Sanft, CFE, Computer Training Specialist SEARCH Group, Inc.

Question 1: In your experience how much of an investigation, digital or otherwise, lies outside the bounds of 'structure'?

- *Briefly discuss the reliance on the talent of the examiner or analyst, dependence on success from other parts of the investigation (i.e. interviews, interrogations, footwork, other non-digital components)*
- *Can the non-structured 'art' of investigation be accommodated in our framework? If so, how might we accomplish the 'art-like' non-*

structured features and tasks? What features of the overall structure would be affected?

SANFT – Checklist and menus are preferred. Talent is not shared nor equal in everyone. There is both science and art, but there should be case-specific checklists, for example, child porn vs. a computer intrusion case. Then there is the difference in media. The checklist must also evolve with time. For example, a floppy diskette found in car wash, marked SECRET might be turned in to authorities, imaged, then the proper checklist might be employed. What type of investigation this becomes depends on the material that was found on the disk. Depending on the severity of the case, certain points may be skipped on the checklist.

HOSMER – With State and Local authorities, the agent is also the investigator. The investigator must posses the skills. Then there is support staff that will collect more evidence to be sent to the investigator later. You can't plan for every contingency nor can you enumerate all the process paths. The judgment of the investigator will be the most important factor regardless of the structure. We may have to deviate from the norm. If, for example, duplication of the hard drive is considered scientific, then the investigation is similar to merely going sequentially through a filing cabinet.

CHRISTY – I have some different perspective of structure in the search for malicious software such as Trojans. We need to go beyond format and display, which are the tools on the market now. Encase, etc. format the display for the investigator to see, but the investigator must still make an analysis. There are no absolutes in the interpretation of the display, so we must reason and take compromises. A structure for reasoning? Is there such a thing? The diversity of the [investigative] team is important, such as mixing people who are CS [computer science] and people who are social sciences. Reasoning with digital evidence is sensitive. For example, a suspect was creating an alibi by changing timestamps. We are looking for a new approach to solving this problem. There are no tools so we have to develop new tools. We can examine the next nearest files to determine if the time stamps were altered.

SANFT – Flying is an art. [Pilots] have checklists also. You would want the pilot to run through the entire checklist first. Similarly, you might want to develop a plan or a strategy of attack or analysis. “Do you plan to find classified information? What are proofs of the crime?” Theses questions will change the path of the plan that you want to develop.

Questions from the floor.

Q: - In reference to the checklists, I have objection to the checklist because in court you will have to defend each item on the checklist.

SANFT: I welcome the challenge. The investigator must logically have reason to fill out something on the checklist. It can all be verified by another tool. The evidence is still there even though you didn’t go through it on the checklist.

HOSMER FOLLOW-UP: Giving a newbie a checklist, they will follow it to the letter. When you get to the higher level of proficiency, you will rely more on faith and experience that you completed the item.

Q: How do you deal with anomalies [deviations] in your standard procedures?

SANFT: You do what you can, and you must document it. There is help available from the higher-level expertise people. Ideally, one problem that was solved a month ago should be documented so that it can be referenced when it is needed again.

Q: Do you put things into phases?

HOSMER: In the learning process, they do not follow these phases (in which they are planned out) but they do take similar steps such as gathering information and imaging it)

Q: How do you handle evidence that the examiner does not have experience in?

SANFT: All agents are computer investigators, etc. If we need to get a different type of expert, we can call upon a financial person, etc.

CHRISTY: ECTF [Electronic Crime Task Forces] – the community of law enforcement and private sector is actively communicating to facilitate this required interaction. There is also INFRAGAURD.

Q: Do you think there is too much art in the forensics process? If so, what can be do to help or hinder the "art" of forensics?

HOSMER: Don't believe there is too much art, and where the line between art and process lie. Hope that groups like this come together for a consensus on the terms.

CHRISTY: This issue was brought up because of the conference and this goes to show the different views people have. Perhaps we take all those different inputs and tie them together somehow.

SANFT: Need to keep up with the changing times. Need the flexibility of having the framework but also being able to modify it when needed.

Q: With regard to art and the investigator, he may keep several premises and jump between several to come to the right conclusion. How do you find a person who can keep track of multiple premises?

HOSMER: Training, instinct, and the inner person who wants to succeed.

CHRISTY: Bring people in from other cultures, languages, psychology, and computer expertise. Don't just take people coming fresh out of training.

HOSMER: Nosy people make good investigators.

SANFT: Involve criminal investigators, and State and Local people who had their own local labs. People fresh out of college should also be part of the mix.

Question 2: It is safe to say that few if any investigations rely solely on digital evidence alone. Sources of evidentiary material usually cover multiple forensic disciplines

- *How can a framework best consider the 'integration' of evidence from various sources?*
- *Comment on the mix (or division) of skills required for practitioners who perform tasks at various stages of the process, so that collectively they can effectively 'integrate' their findings.*

HOSMER: This question was covered in our discussions for the last question. The more complex a mix, the better the team. It is important to be able to go out and ask someone else for help

CHRISTY: Everyone has their own specialties. You will need to expand your own knowledge base working with other people. Criminals get smarter. [An example is the criminal who starts] putting child porn on an Xbox, while the investigator who comes to collect evidence will ignore the Xbox. You will always need to learn more and build better tools, faster. [From now on we must] come to conclusion that this computer user is smarter than we think, and must assume that the suspect has other means of storage (such as the Xbox) [when we investigate.]

SANFT: Examiners must communicate with the case agent. Three people: victim, forensic examiners, and prosecution. They must all communicate to get the best result. An opportunity to do that is the DoD Cybercrime Conference. Invite the law enforcement, prosecutors, and examiners to come together and share ideas.

Audience [Mark Pollitt]: There are those people that will want to get their hands on everything. Have to balance the personality traits vs. investigative goals. Goal is to prosecute that case. Traits examples are being aggressive, "making it happen", etc. Investigators' long term goal is a "technical exercise". You want someone who is methodical and meticulous. Professional analysis would put together the puzzle just for the sake of saying that the puzzle is complete.

Audience [Jack Mineo]: Given a bag of tools and a smart guy, they will solve the problem. Ex: The wrench mechanic sees an indicator and tries different tools to fix the problem. In the cyber world, we would need people (engineers) to "predict" the indicator and look for it (the premise). Then, we will need the bag of tools or maybe a new bag of tools. And the main factor would be technology.

SANFT: The case agent (in DCC lab) takes the evidence gathered from all the different labs and puts it all together.

Q: What are the challenges of going cross-discipline in our investigations?

SANFT: The little "R" and the little "D" [in R&D] because of the little dollars. Goal is to work [make investments] on existing tools instead.

CHRISTY: Just trying to understand all the cyber tools is a huge resource user. We have to rely on other people who already have the skills and then learn (and keep) the knowledge from that experience.

Question 3: The digital forensic community is growing almost exponentially. Our efforts here are only part of any potential solution path. What are some recommended private, Federal, DoD, or international organizations that our group should be collaborating with to evolve an accepted digital forensic investigative framework?

- *In your response, consider the investigative utility of having similar frameworks or processes between organizations that work together (e.g. DHS and DoD, DHS and FBI, etc.)*
- *Comment briefly on the process through which proposed frameworks would be vetted by the organizations you recommended.*

[RESPONSES WERE TIME-CONSTRAINED]

HOSMER: Everybody and nobody. There is probably a huge interest in this topic, but the resources and time needed to find all these other organizations and group is extremely difficult. State and local,

federal, academia, etc, all have various backgrounds to compound together.

CHRISTY: There is no framework for communication between all these groups. The framework is driven by the market and vendors. We need to change that. Vendors are pushing out new tools and we have to take them and use them.

Audience [Brian Carrier]: We need to be collaborating on SOPs [Standard Operating Procedures] instead of having common frameworks. Each lab has their own SOP and we need to integrate them all.

Workshop Sessions – Foundation for a Framework

The remainder of Day 1 was devoted to concentrated workshop discussions. The workshop topics were chosen to stimulate dialog in the areas related to the continuing evolution of a generalized Framework that could be applied to nearly every investigative domain. The following list summarizes the categories of topics addressed in each.

- Future Framework Directions
- Role of Technology as an Enabler/Disruptor
- Application of Framework to Investigative Environments
- Pathways to Framework Adoption

In addition to expected dialog, the group discussions uncovered new, unanticipated challenges as well as potential approaches to problem solving. However, the groups focused primarily on the following foundational issues regarding the framework:

- Determine the structure of the framework
- Identify the technologies necessary for the framework
- Application of the framework
- Community communication and organization

Attendees were divided into five groups. Each group was assigned a topic and discussion took place for approximately two hours, during which time each group prepared charts to describe their findings. After group interaction was completed, each group presented its briefing to all in attendance and followed up with a question-and-answer period. This approach allowed for a variety of perspectives drawing from the wide spectrum of knowledge and experience levels in each group.

Each of the following workshop descriptions begin with a notable quote/conclusion from each group, followed by a listing of the topics to be debated, a description of where the group focused their efforts, points of deliberation, and concluding remarks.

Breakout Group 1A/B – Ideal Structure and Expertise for Investigation

> ***"The physical and digital world models are already merged; it is merely the techniques for investigation that are different."***

Topics to be Addressed:

These two groups independently considered the single best structure from a combination of what had been presented as well as other sources as appropriate. Participants were encouraged to merge, reevaluate, innovate as necessary. They also considered how well the ideal approach accommodates different investigative domains, and they assessed the models' ability to integrate digital evidence with other forms of proof

For each stage of their ideal model, this group outlined the specialized skills required for, keeping in mind that some areas of expertise may bridge stages. An attempt was made to name and define the specialty area in terms of an existing title, or develop a new title, if appropriate (i.e. imaging/digital preservation – file system analysis – event reconstruction – digital artifact analysis – hidden data recovery, etc.). When feasible, this group developed an outline of competencies and potential certifications required for each specialty area.

Group 1A Leads

Facilitator: Dario Forte, Digital Forensics Lab of Italy

Recorder: Tanya Allen, AFRL

Group Focus

The main focus of this break-out group[1] was on the difference between the old framework versions versus Brian Carrier's model. The group believed that one of the main factors guiding model selection was the importance/role of preservation, since preservation's emphasis varied between models. For example, one question that arose was "Does [the]

[1] Participants were Dario Forte, Frank Adelstein, Tanya Allen, Nicole Beebe, Cheryl Brown, Ian Bryant, Raj Chauhan, Larry Coffman, Marty Gray, Lorenzo Martignoni, Jim McIntyre, Mattia Monga, Roy Nutter, Eric Ozanam, Kelsey Rider, Todd Shipley, Christopher Williams, and Laura Wood.

intelligence [community] need Forensics [in its investigation process]?" This question resulted in a consensus that it all depends on how a particular community of interest views the definition of forensics. Other topics of consideration dealt with the relationship between Digital and Physical Evidence, as well as "Who is required and has the skill set to perform digital forensics?"

Overview of Group Deliberations

The group decided that each COI needs something different out of the forensic process, so one particular framework will not work for everyone. In light of the disparity in views of what is required for data preservation, the group first decided to define what exactly preservation is:

- Preservation: ensuring the availability of data and information , when possible and when needed [e.g. in the manner for which it is needed.]

Some of the key considerations that the group reported while discussing preservation issues were as follows:

- Keep what you need and don't go crazy – decisions on what to keep could ultimately affect the quality or timeliness of the investigation.
- Courts limitations are influencing the amount/volume of evidence that can be considered, and how timely of a manner it must be analyzed.
- Preservation is important to all, but its mechanisms depend on the COI's meaning/intent of preservation as it relates to the COI's framework or investigative process.
- Integrity must be assured in preservation process.

The different goals of the various agencies determine the role of preservation. Law Enforcement has a high need for preservation and integrity, while commercial businesses may not be as concerned with preservation. Furthermore, there was discussion {based on Beebe's presentation?} concerning the use of a matrix that would include the various methods needs for preservation, which could be a selectable

attribute of the framework. However, this discussion did not result in any single best structure.

The second topic of discussion was the physical world of evidence vs. the digital world of evidence. The question discussed was “Is it possible to merge the physical and digital world in the investigation process?” In other words, were there nuances to investigating the digital realm that make it unsuitable for the same processes of the traditional physical realm? The conclusion was that digital evidence is merely a special case of physical evidence, and that they are really both from the same realm. However, it was noted that in the physical world, small errors equal small errors [due to the analog measurement techniques used to measure footprints, tire skidmarks, etc.], while in the digital world, a small error [e.g. the flipping of a significant bit in a piece of data] could result in a significantly large discrepancy [due to the discrete mathematics of computers]. As long as these differences are kept in-mind, the “mental approach” and process to analyzing digital evidence can be the same as the physical one, and can lead to merging of the investigative processes. This conclusion echoes one of the DFRWS2001 outcomes, indicating that the original work provides a stable foundation for further framework development.

In the limited time remaining, the group briefly discussed the minimal desired skill set for certifications as a digital forensic investigator. The following recommendations were made: Certification itself (passing a knowledge test) is not the desired end state. Rather, it is the demonstration of competency or proficiency as it applied to the investigative environment, and is enhanced with skills and experience. By the same token, a university degree for a forensic examiner would not be necessary either, (as it probably wouldn’t go far to demonstrate skills and experience). The question remained: “Who, then, would validate this measure of competency?” The examiner should be able to measure the following factors:

- Knowledge, skills, experience
- Desired training, according to a checklist

Possible competency fields could be:

- Digital Evidence Technician (Responsible for initial handling of evidence, and creating forensic duplicates. This person has no investigation skills in addition to his technical competences)
- Digital Investigator (at least 3 years of experience, general knowledge of the digital forensic and investigations processes)
- Forensic Examiner (at least 5 years of experience, highly technical and specialized skills)

Who can be entrusted to establish the standard in general? Perhaps the various collective COIs, in general, with the advocacy/support of NIST. NIST is perceived to have been an independent, impartial party in this area, and might be accepted in this role.

Concluding Decisions

The group concluded that there will/should be a general framework that COIs or individuals could modify to suit their own specific investigative needs. Furthermore, the role of preservation is a significant guiding factor in the establishment of process and framework. Lastly, there are some important considerations for how we might verify the credentials and experience of digital investigators. The experience will often depend on the environment they are working, or a particular community's needs. There may be an opportunity here for developing core training attributes in order to produce (as well as attract) better digital investigators.

Group 1B Leads

Facilitator: James Lyle, NIST

Recorder: Scott Rey, AFRL

Group Focus

This group[2] contained a significant law enforcement/practitioner influence, which may attribute to the alternate findings depicted below. Although there was a lot of discussion and ideas thrown around, the group was unable to converge on a single best framework. Instead, the group spent time critiquing the ones presented during the morning session.

Overview of Group Deliberations

Some initial discussion about the role of framework included:

- Framework exists simply to show process. It does not need to go into detailed procedure.
- That being said, an investigator can't treat every case "by the book," since each case has its own nuances. Incorporating all features of a process will take a very long time for an investigation, and may not be responsive [to the perishability of digital information] or other time constraints.
- Most investigators get the information they need right now and worry about whether or not it was "done right" later. Using this argument, it could be concluded that on its own, a framework does not buy us anything. It just simply helps to advance the field philosophically.

Taking these guiding thoughts in mind, the group had the following comments on the suitability/features engendered in the morning's briefings toward an ideal structure/framework:

- **Nicole Beebe's**: with all its sub-phases, this framework was thought to be too deep and there is not enough breadth.

[2] Participants were Art Conklin, Gary Gordon, Yong Guan, Mark Hirsh, Albert Holt, Brian Kropa, Jack Lewis, Jim Lyle, Scott Rey, Golden Richard, Mark Rose, Scott Stipetic, and Florence Tushabe.

- **Mark Pollitt’s**: was very law enforcement oriented. The ideas need to be more objective driven.

Concluding Decisions

The overall conclusion for part 1 (creating a framework) resulted in the decision – “We believe our models will evolve with time and will be published in journals and debated,” [with not much utility to be derived by the practitioner community.]

Breakout Group 2 – Framework Technologies and Maturity

> ***"Frameworks should be technologically-independent, and perhaps should aim only for the '90% Solution' in meeting most investigative needs, as meeting all needs is improbable."***

Topics to be Addressed:

This group considered the outlying or novel framework stages that were presented, and the unique capabilities required for them. In addition, an effort was make to identify technologies that could prove useful in providing these new capabilities, including but not limited to: hardware, database, client server, data mining, radio-frequency identification (RFID), handheld-wireless, encryption, etc. When feasible, definitions were established for each technology in terms of forensic significance and technological maturity vs. how much research is still necessary. An effort was also made to design a technology "data flow" or data inter relationships among technologies within a major category, between categories, and to other external investigative sources.

Group Leads

Facilitator: Eoghan Casey, Stroz Friedberg LLC

Recorders: Heather Dussault, SUNYIT; Thomas Parisi, AFRL

Group Focus

This group[3] reviewed the papers presented earlier in the day and focused on the more challenging processes in digital investigations and issues pertaining to technology and how it affects frameworks. The discussion started with a short list of challenges that might exert the frameworks: anonymity, wireless, mobility, concealment, differences between physical and digital crime scenes, evidence in networked systems, and the causes or effects of events may not be resident locally. Potential technological solutions to some of these challenges

[3] Participants were Eoghan Casey, Brian Croniser, Kyle Dempsey, Heather Dussault, Chet Hosmer, Jordan Jacobs, Chris Lefever, Steve Mead, Chris Sanft, Kulesh Shanmugasundaram, Mike Sieffert, John Tebutt, and John Ward.

were then discusses. However, from the outset, the group stipulated that the framework should remain technologically neutral in that the framework should not specify a particular piece of technology that should be used during the digital investigation.

Overview of Group Deliberations

This discussion began at the beginning, considering the initiation of a digital investigation. The question, “How are we equipped to deal with the digital crime scene?” was raised, which led to a discussion about the commonalities and differences between the digital and physical crime scene investigation. It was agreed that in both traditional and digital crime scenes, investigators often have a tendency to look what we are looking for. One of the primary purposes of the framework is to help investigators break out of our preconceptions and increase the likelihood that we will find the unexpected rather than simply look for fulfillment of what we expect.

However, a framework can only go so far. The investigator will need to determine the expertise of the suspect to ascertain the appropriate application of analytic techniques. The knowledge and experience of the investigator will determine questions like, Has the suspect used data hiding techniques such as steganography?, Has the suspect used encryption?, Can we break the encryption or just ask for the keys? Ultimately, criminals will continue to “adapt” to our methods and tools. We must be creative and remain one step ahead of them, which will inevitably compel us to applying forensic principles in new situations and possibly extend the framework.

The group elaborated on difficult stages of digital investigations, ranging from general issues such as identifying a larger context for the investigation and inputs into the framework, to specific concerns such as the ability to locate hidden information, malware, stegonography or other concealed information and breaking into it if we find it. The difficulties of dealing with dynamic situations were discussed, as well as identifying a user’s level of sophistication and level of paranoia.

Technological Needs

The group then considered what needs currently exist for an investigator at a digital crime scene. What questions are asked, and how can they be technologically addressed? Evidence preservation at the digital crime scene is crucial, but is also resource intensive and draining. The consensus of the group was that the technical gap which hinders efficiency lies in both software and hardware. For instance, complexities and sensitivities of system Input/Output can slow down or prevent evidence acquisition and in some cases can cause inadvertent changes to the original evidence. This raises a concern about the ability to acquire, store and examine large amounts of data in a reasonable amount of time – will technology be able to address the exponentially growing disk capacities?

Developing specialized hardware for certain tasks could address some of these issues. For instance, manufacturers integrating write blocking at the hardware level of all storage media could eliminate the need for a separate write blocking device. Changes to our acquisition methodology may also be needed, such as increased use of filters such as hash sets, filtering during acquisition, and data previewing rather than acquisition in more cases. If human investigative processes were modeled and developed into intelligent preservation tools, it may be possible to capture the majority of useful digital evidence efficiently from a large number of systems without taking a full memory dump and disk image. This could also enhance remote pre-imaging examination capabilities, intelligence gathering tools, and could help deal with the masses of data and backlog of imaging work in labs

More effective tools for data mining and performing reconstruction and profiling might also help extract useful information from large amounts of data more efficiently. However, as tools become more powerful and sophisticated, there is a risk that they could become more error prone. There is a need to maintain the reliability and repeatability of their processes.

The discussion of partial acquisitions led to a comparison between a physical “paper trail” in a civil case vs. a digital “paper trail.” If physical papers were seized, only incriminating files are taken, not the whole office filing cabinet. The main risk of partial data

acquisition is that relevant evidence might be missed, particularly if it was intentionally concealed. This speaks to a need for better ways to detect hidden data. However, in some situations we are only getting a partial acquisition. For instance, when examining some mobile telephones or personal digital assistants, current tools can only acquire a portion of memory. Similarly when performing live examinations either at the console or remotely, it is only possible to obtain a snapshot in time, which in itself can be viewed as a partial acquisition. In any event, to create a "paper trail," it would be useful for an investigator to have tools that create a log of all actions that can later be admissible in court as evidence.

Challenges faced in network forensics

The group also outlined the need for technology to address the following issues relating to networks. One challenging technological issue mentioned was trace-back ability especially in a wireless environment. There is a possibility of false identity over a network through MAC spoofing. In one case involving wireless access points, it was not possible to attribute criminal activities to an individual using digital evidence alone. It was necessary to combine traditional investigative techniques and surveillance with the digital evidence to apprehend the offender. This also demonstrates that time and locality plays a crucial role in network forensic applications. Investigators had to follow the primary suspects for several days and then correlate their findings with digital evidence from the same periods to determine which individual was in a particular location at the time of the crime.

Free mail and "hush mail" provide some level of anonymity but, with the proper tools and training, investigators can attribute activities to an individual and even use the non-repudiation properties of public key encryption to implicate a particular person.

Some participants suggested that recommendations should be made to software and hardware vendors, to integrate the ability for network forensics into their products. However, this was not a majority consensus and some argued that we should not try to change the world to suit our needs.

Hard Technical Problems in Framework Tasks

Intelligence	**Modeling, Modeling Languages, Profiles, new analysis "algorithms," capturing expert knowledge in knowledge bases** **Event drive, evidence driven, historical knowledge** **Intelligence could help address more fundamental issues e.g., data reduction**
Remote	**Remote triage, access and imaging, networks**
Preview	**Improved methods of triage, possibility of incomplete information with network drives / missed evidence**
Filter/Data Reduction	**Hash sets (band-aide?), data reduction**
Hardware	**Write block integration, hash calculation processor (for speed improvements), freeze OS for a true preview, self-auditing tools for dynamic analysis (e.g., decrypting EFS)**

Concluding Remarks on Framework

The group consensus was that there is a need for different frameworks to account for different investigative scenarios. There should be one framework to address the "dumb" criminal, while there should be another to address the "smarter" criminal in a time-critical investigation. These two sub-frameworks should originate from a single main framework. The sub-frameworks can be viewed as a framework having only a subset of the processes outlined in the main framework. The ability for new sub-frameworks to appear leads to the idea that the final proposed framework should be dynamic so that it can be adapted to solve unique problems.

When applying technology to a framework, we are probably looking only for a 90% solution that will apply to nearly all investigator's needs. We need to consider approaches other than the 'make no mistakes"

frameworks, which are often inefficient and untimely. In addition, since each case is unique, we need to be dynamic and adaptive in our processes, and as well, need to share information more intelligently between process steps. However, there is the potential for increased efficiency and reliability if aspects of the framework are embedded in our tools. In the same vein, when applying tools or technology to a framework, we need to understand how a framework or process may already be embedded in the capability. Knowing this will help make better decisions about how to apply the tool, or when using the tool will actually make the task more difficult. There is an incredible opportunity to apply data mining and data associations to the digital domain, as well as in multi-domain (physical) investigations. This correlation of information alone could help drive an evolution in framework/process.

As we progress, it is important to keep in mind that our solutions may create new challenges. For instance, as our tools become more sophisticated, it may become more difficult to explain how analysis performed, and to accredit or certify tools.

Breakout Group 3 – Applying the Framework to Multiple Domains

> ***"Framework should not specify processes and steps, but rather, it should contain categories that should be followed to mitigate liability, akin to the software capability maturity model."***

Topics to be Addressed:

This group considered strengths and weaknesses of each model's applicability to various investigative environments (e.g., law enforcement, intelligence, corporate, military, homeland security, etc.). They considered storage media, network, and other potential forensic domains. Special consideration was given to framework suitability and adaptation in operational or "live" environments.

A related set of questions that this group considered dealt with the degree to which these models challenge the current investigative model. What are the hurdles to implementation? Does the model require different, perhaps more complex or demanding skill sets? Is there questionable support to admissibility?

Group Leads

Facilitator: Gary Palmer, MITRE

Recorders: Mark Williams, AFRL; Nelson Lee, AFRL

Group Focus

This group[4] started the discussion by considering the limits of each model and how they would apply to each organization. The group had also determined that in order to apply the framework, they would need to look at the following fields: law enforcement response, legal defense response, and the investigation process. For example, the investigative process that the group performed comparisons with was the FBI search and seizure model.

Overview of Group Deliberations

Existing models and how would they be challenge

[4] Participants were Gary Palmer, Venansius Baryamureeba, Jim Collins, Mike Duren, Dave Lang, Justin Levinson, Pat Logan, Nelson Lee, John Lowy, Lance Spitzner, Hong Zhao, and Mark Williams.

The FBI Search and Seizure model is a well known and field-proven process. The goal of the DFRWS workshop is to get the reputation of a new forensic framework to this level of recognition. However, the problem lies in establishing the link between a theoretical framework to one that is practical. In order to address these problems, we must address the following items:

- Consider the little people. Smaller organizations do not possess the equipment, manpower, and resource compared to larger scale organizations. They require the flexibility that needs to be offered in the framework. For example, the flexibility to complete certain required processes in the framework.
- The framework should have categories instead of specific processes. For example, “evidence gathering” can be considered a category, but the process and procedure of collection will not be specified.
- Rank the environments on a numeric scale. The higher an organization’s rank or level, the more categories it can accomplish in the framework for a given investigation.

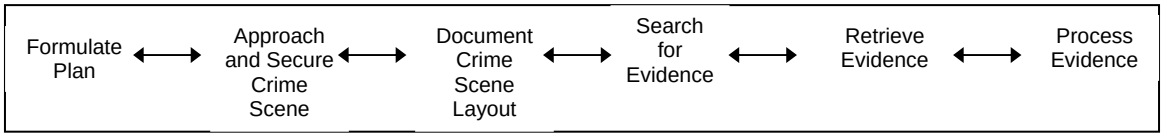

Figure 6 - FBI Investigative Model

Proposal for a “Capability Maturity Model (CMM)”

During the discussion, the group had decided to compare the structure of the framework to that of the Capability Maturity Model (CMM). The CMM specifies 5 unique levels that an organization or company must achieve for software engineering practices. In short, the higher the level, the company is more mature and developed. This serves to add credibility to their name.

The idea is to somehow port the concept of the CMM over to the Framework idea. We can use levels (0, 1, 2,...) to rank, rate, certify, and validate a certain phase. Each phase or category can be ranked, and the lowest score will be the overall ranking.

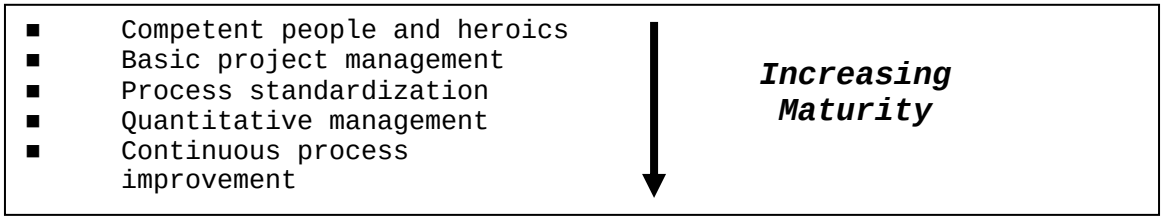

Figure 7 - The CMM Model

The idea of having a framework where the processes are ranked may address the following issues:

- Whether the computer investigation can be admissible to court.
- How good is the evidence?
- A maturity standard.
- How in-depth was the evidence analyzed?
- Both sides in a legal battle should be able to follow the steps of “maturity”

Admissibility in court

The purpose of having a framework is so that steps [minimal requirements] can be checked and validated to be complete. If the proper steps are taken, then no false or altered evidence should be improperly or inadvertently introduced into the investigation. The following points were mentioned during discussions:

- Courts do not like “openness” in a framework where there are different steps and frameworks. The goal should be to form one framework which is flexible enough to change or adapt to conditions.
- Even though all steps in the framework were taken, you can still argue the reputation of that evidence. It is up to the defense lawyer to argue against the credibility.

- The steps in the framework should be designed to cover your liability. For example, if you did not follow a step, then you should argue from a lack-of-resource point of view, instead of saying you forgot to complete that step.
- Courts want truth and credibility of admitted evidence

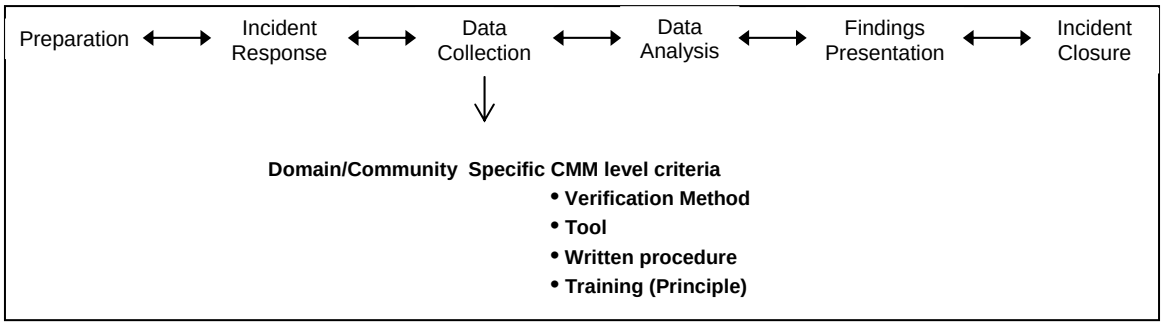

Figure 8 - Proposed Application of CMM Criteria

Concluding Decisions

The following example summed up the consensus of the group's discussion. Ex: Cleaning your hands before an operation doesn't say what type of soap needs to be used. However, if later it is discovered that you caused an infection that led to the patient's death, you will be held liable. Analogous to the framework, it should not specify processes and steps (the brand of soap), but the framework should contain categories (washing of the hands) that should be followed to ensure quality and mitigate liability.

Breakout Group 4 – On the Path to Adoption

> ***"Developing 'measures of merit', for the purpose of demonstrating process efficiency [over current processes being employed], may be the most important factor in our ability to get community buy-in for a particular framework or process."***

Topics to be Addressed:

The group was to build and document a plan for community dialog that will lead to adoption and use of a Framework for digital forensics. The group was asked to cite other groups and organizations should be involved, considering on-line communities, and private, professional, and government orgs. When bringing together people, building the community, or disseminating information, try to determine what forums will work best, for example, workshops, on-line forums, list servers, or through publication? What is a realistic timeframe for adoption? Finally the group was to outline recommendations for how this new adoption approach may be integrated and adapted for use, including any ideas related to education, training and what it may require for competence.

Group Leads

Facilitator: Mark Pollitt,
Recorder: Chet Maciag, AFRL

Group Focus

As a starting point for discussion, the group[5] first explored what the value of a framework would be to a given community of interest. It was concluded that interest in a framework stemmed from 1) Philosophical; 2) Theoretical; and 3) Practical angles, depending on whether you come from the judicial, academic, or practitioner point of view. In order to gain adoption of a single generalized framework, it is necessary to understand what each audience wants from the framework. That, in turn,

[5] Participants were Mark Pollitt, Edward Balas, Paul Blythe, Brian Carrier, Jim Christy, Natalie Harrison, Jim Jones, Benjamin Long, Chet Maciag, Jack Mineo, Bob Pasquarella, Phil Turner, Thomas Parisi, Pete Ware, and Doug White.

will help to drive selection of the advocacy or adoption method applied within that community.

It is also necessary to help educate the potential adopter or community on the advantages of adopting a new framework, such as improved timeliness, efficiency, and step traceability, in order to gain critical mass. This is particularly true of the law enforcement community which, for good reason, attempts to make evolutionary rather than revolutionary changes to process in order to minimize risk in the presentation of evidence in a legal venue. Unfortunately, this can be a difficult proposition, since investigative framework can serve as the foundation for business process within an organization, making it very difficult to "try before you buy". Instead, the curious are forced to take substantial risk in process reengineering, often with the potential for incompatibility and skepticism from other community agencies.

Also, on the path to framework acceptance, the group explored the difference between frameworks, standards, and best practices. Which would be the best approach for achieving the general intent of developing common techniques and capabilities between organizations? Unfortunately, the group found a fuzzy line between what might be considered a standard, best practice, and investigative framework, as presented earlier in the day. For example, it was difficult to explain the difference between the framework (overall process) and best practices (specific accepted procedures) vs. standards (which could specify either). As a result, the group provided the following prerequisites that should be considered prior to promoting a particular framework:

- Global adoption of a framework may not be the only measure of success. If there are several frameworks, and each widely applies to a particular community, then success might also be realized.
- It is probably even more important to understand how to apply a framework than it is to know the framework. In many cases, a general framework should be tailorable and scaleable to meet

a particular investigative need. Each case might not require all facets of the framework.

- If you value the use of best practices and specially-trained individuals, the adoption of such certification criteria may be for you. ASCLAD is one such example, and could override the need for a common framework, depending on the application.

Overview of Group Deliberations

That being said, the group still was able to define several benefits from developing a framework:

- The framework is a starting point for the identification, comparison, and production of tools/capabilities across Industry and Academia. It includes functions that comprise a digital forensics investigation, as well as its relevant processes.
- It serves as a context for the use of tools/capabilities
- It can define a meta-standard for describing what features should be included in a standard. Alternately, it could be viewed as a guide for building standards (akin to ISO 17799, an organization would be certified akin to ISO 900x in Industry.)

In defining a process toward acceptance of a framework, the group considered the scenario in which they were the recipients of a framework that was being peddled. They had the following comments about how it would be received, and the difficulties experienced in implementation:

- A framework will be accepted only over a period of time, after demonstrable results, and that will take time.
    - However, trying to do that prematurely runs the risk of running against what ultimately will be determined to be the best practice.
    - Hard problem: How does the proponent of a framework demonstrate this quality of “demonstrable results?” Unfortunately, since framework/process is so closely

tied to business function, it is difficult to “try before you buy”, yet impossible to really measure increased value if you don’t actually try it.

- Methodology that is properly developed and applied will be iterative in development and will help to drive technology, and technology will help to drive innovation in the methodology. This should be an ongoing process for improvement [remember Group 3’s brief on the role of CMM?]
- Consider “What should the intended impact be on the potential adopter and/field?”
    - As a result of this, we may be able to work backward to define the organizations that would have a vested interest in a given framework.

Concluding Decisions

In conclusion, the group decided that the keys to stimulating adoption of a framework are:

- Improved articulation of what a framework is (e.g. Standard, Meta-standard, or Process?) so the ‘buyer’ will recognize it as something that they need.
- Developing measurable ways to define the added value or limitations of a framework. Without these measures of merit, we cannot engage in any fruitful discussion with a potential recipient. Developing metrics of efficiency, timeliness, and reliability are a significant challenge.

Day 2 – In Time Forensics

Introduction (From the Call for Papers)

We have before us an important opportunity to discuss potential solutions that enable us to review data collection and processing approaches in terms of responsive “In Time” applications. “In- Time” refers to the development of approaches that factors time along with evidence importance into the overall data collection, correlation, analysis, and decision process. This view affords consideration of forensic science and its applications to the widest spectrum of investigative domains, all who must consider overall response time, but, all who use vastly different criteria with respect to time. It also focuses on time as a critical systems/architectural issue, versus just measuring time based on current process or technology capabilities.

As the worldwide collaborative paradigm for Homeland Security is being realized, investigative domains must find the most effective common ground for successful collection, assessment, communications and decision-making. Once separate processes serving disparate law enforcement, military, national intelligence, and private sector operations, they must now join forces to this end. They must search for a mechanism to share technology, data, factual knowledge, and information to combat growing, increasingly sophisticated global threats. Forensically sound, validated facts delivered “In-Time” forms the nexus for this collaboration.

The forensic combination of factual evidence and its associated statistical confidence is at the heart of all investigations. What differs most clearly across investigative domains (military, national intelligence, law enforcement, and business) is the amount of time those involved may wait to analyze and deliver that evidence. A wide variety of factors drives this difference including, legal guidelines, mission criticality, prosecutorial time constraints, required transaction rates, and system availability just to name a few. Although these differing perspectives, and the fact that they exist,

were discussed and documented in the first DFRWS (2001), implementation details are still being sought.

In many respects, the general data collection issue has been satisfactorily addressed. Large quantities of unclassified information from a wide variety of personnel stores, communication sensors, and various other databases are widely available. A significant portion of the challenges that remain pose much harder problems. The technical areas of data fusion, correlation, reasoning, visualization, and otherwise detailed forensic analysis pose a serious technical hurdle for us. Integration of these developed technologies employing systems/security engineering and architectural approaches that meet the varying needs of varying investigative domains may be an even harder task. Coupled with the ultimate goal to securely communicate or share the reasoned findings, we see that much work is left before we can hope to jointly confront global threats effectively.

Response time, as a criterion, is a critical and essential component that differentiates what forensic technologies can be applied across the spectrum of users in digital forensics. Today, we will explore, debate and document the time requirements associated with different domains and perspectives that use or are considering the use of forensic tools and technologies. In addition, we will consider approaches to mapping the time criteria to the candidate Framework for Digital Forensics (from Theme I).

Keynote Presentation

Lance Spitzner, “Honeynets and Digital Forensics”

Mr. Spitzner discussed the challenges of near-real-time forensic in operational environments, starting with the question, “How can we defend against an enemy, when we don’t even know who the enemy is?” And when we do, the threat’s tactics and techniques change rapidly, making it difficult to keep pace. He proposed one possible solution – learning more about malicious intruders and sharing the knowledge. The Honeynet project created by Spitzner fits with this solution by

providing information and enabling research about attacks and the behaviors of intruders.

The Honeynet Project has three main goals: Raise awareness that threats exist, inform how to deal with threats, and increase the capacity for research with academia. Awareness seems to be one of the most important factors, as most people don't seem to realize that they are a lucrative target or intermediary pawn, in the eyes of criminals.

There are three main challenges to investigating live computer systems: Data overload, amount of time to analyze, and experience required to analyze. Data overload is one of the most daunting challenges, particularly when correlating data from multiple systems. Data reduction and prioritization is possible with Honeynets, as all activity destined for a honeypot is automatically deemed suspicious (e.g. only 'needles' are received – there is no 'haystack'.) Still, Substantial time and expertise are required to analyze all of the data. And this problem will get worse as the Honeynet Alliance shares information among its members around the world, however, the payoff of a more complete global picture will be worth it.

Table 2 - Honeynet Alliance Members

• South Florida Honeynet Project
• Georia Technical Institute
• Azusa Pacific University
• Paladion Networks Honeynet Project (India)
• Internet Systematics Lab Honeynet Project (Greece)
• Mexico Honeynet (Mexico)
• Honeynet.BR (Brazil)
• Irish Honeynet
• Norwegian Honeynet
• UK Honeynet
• French Honeynet Project
• Italian Honeynet Project

Currently, a team approach is required to effectively perform such tasks as analyzing file system activity and processes, network traffic, human behavior, and reverse engineering. Even multiple language skills are required to understand this global activity. However, there is a limited number of skilled people. Therefore, more automation is needed to offload as much of the data processing as possible from skilled people and to minimize the amount of experts that are required for each investigation. Better GUI tools, databases of clean and hacked images, and reduction of data using MD5 hashes will still be key enablers in focusing only on new and changed information on the system being analyzed.

Plenary Speakers

Several presenters outlined approaches to preserving and examining data on live systems.

Edward Balas, "Honeynet Data Analysis: A Technique for Correlating Sebek and Network Data"

This paper presented a component of the Honeynet project, called Sebek, which automates the correlation of host and network data to provide a more complete picture of events during an intrusion. Sebek is also used on the honeypot/host, in order to capture and record keystrokes and related activities when session encryption is used, and otherwise is not readable by network IDS systems. Current Sebek capabilities and limitations were described, as well as future wishes for ways to automatically screen, coalesce, and report recorded information for the human. Capabilities of other Honeynet tools, Hflow and Walleye, were also presented, which assist in coalescing data and providing unified views of network flows and events.

Heather Dussault, "Forensics, Fighter Pilots and the OODA Loop: The Role of Digital Forensics in Cyber Command and Control"

This intent of this presentation was to draw an analogy between the time-sensitive requirements of traditional airborne dogfights and cyber investigations involving forensic analysis. Col John Boyd’s 1987 paper on Observe-Orient-Decide-Act (OODA) loops served to explain why older U.S. fighter technology outperformed advanced Soviet fighters in dogfights: It was the ability to take in, assess, decide, and act upon a given airspace situation faster than the adversary. The human-controlled interface of U.S. F-86 fighters allowed them to respond faster to a threat than the more automated Soviet Mig-15.

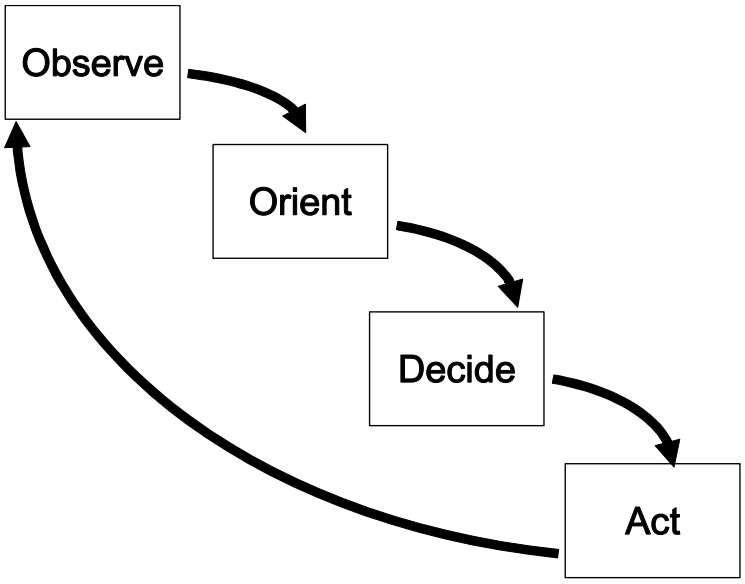

Figure 9 - Boyd's OODA Loop

The need to respond in a manner timely to enemy threat is similar to our objectives in cyber defense operations, where quick reaction times are required to keep pace with the adversary to preclude loss of precious situational awareness, traceback, or attribution data, and where cyber 'dogfights' might only last a mere few seconds. By contrast, current measures of timeliness in digital forensic analysis are on the order of weeks and months, depending on the level of integrity required for collected data.

If the OODA loop is how fighter pilots measure timely command and control, then the Protect, Detect, Assess, and Respond (PDAR) is the model by which the AF performs command and control of its computer networks. Like the OODA Loop, it is also iterative in nature. A mapping of digital forensic science processes into each command and control model is as follows:

Table 3 - Mapping of Forensic Processes to OODA and PDAR Models

Digital Forensic Science Process	OODA Loop	PDAR Cycle
		Protect
		Detect

Identification	Observe	Detect/Assess
Preservation	Observe	Assess
Collection	Observe	Assess
Examination	Observe/Orient	Assess
Analysis	Orient	Assess
Presentation	Orient	Assess
Decision	Decide	Respond
	Act	Respond

Note that in this mapping, none of the digital forensic process functions map to the OODA 'Act' function. This may be reflective of forensic investigations not being thought of as a 'dogfight' in which there is a need for rapid action. Hence, the processes and techniques that we currently employ will probably not be built for timely response either, which is a problem since cyber threats require rapid responses.

Some opportunities for implementing digital forensics in cyber command and control systems include the following four areas: (1) Forensics for planning, where response courses of action are developed based upon law enforcement scenarios and lessons-learned. The plan can be red-teamed ahead of time to ensure exit objectives are met by the plan. (2) Forensic support for rapid decision-making, where the criteria for data fidelity and accuracy is established in advance of an incident and subsequent analysis. (3) Forensics processes in predictive battle/defense management, where system and adversary behaviors and responses are forensically analyzed and predicted based upon scientific methods. This is a key enabler for getting inside the adversary's OODA loop, because we can rule out unlikely or impossible adversary future courses of action more quickly. This can also help expedite battle damage assessment by ruling out what information systems could not be affected.

Departing observations were that success will be based on identifying, in advance, minimal essential elements of forensic information for cyber command and control. The solutions that we develop (process or technology) will eventually have to be scalable to large numbers of

systems in order to be effective. Finally, challenges exist in developing continuous forensic analysis techniques for time-sensitive environments (e.g. where hypotheses are continuously evaluated over time, to help predict events before or as they occur.)

John Lowry, "Adversary Modeling to Develop Forensic Observables"

This paper addressed the difficulty of reacting to adversaries rather than being equipped to anticipate their actions, and outlined an approach to modeling adversaries. All previous attempts at detecting malicious cyber behavior fail to include a priori development of observables. A posteriori methods not only fail to detect novel attacks, but generate observables that are over-specified, and are therefore difficult to generate and keep up to date. Other defensive resources will become exhausted or ineffective.

A priori methods rely upon threat modeling in an attempt to develop the key observables. Potential adversaries and their malicious acts are hypothesized. From there, threats and adversarial missions are identified, along with their corresponding means of attack and the probability that each one would have been used. Finally, observables are developed for each of the identified avenues of attack. In this way, detection is focused on detecting the adversary’s desired effect, rather than on a particular fine-tuned signature that corresponds to a specific attack method.

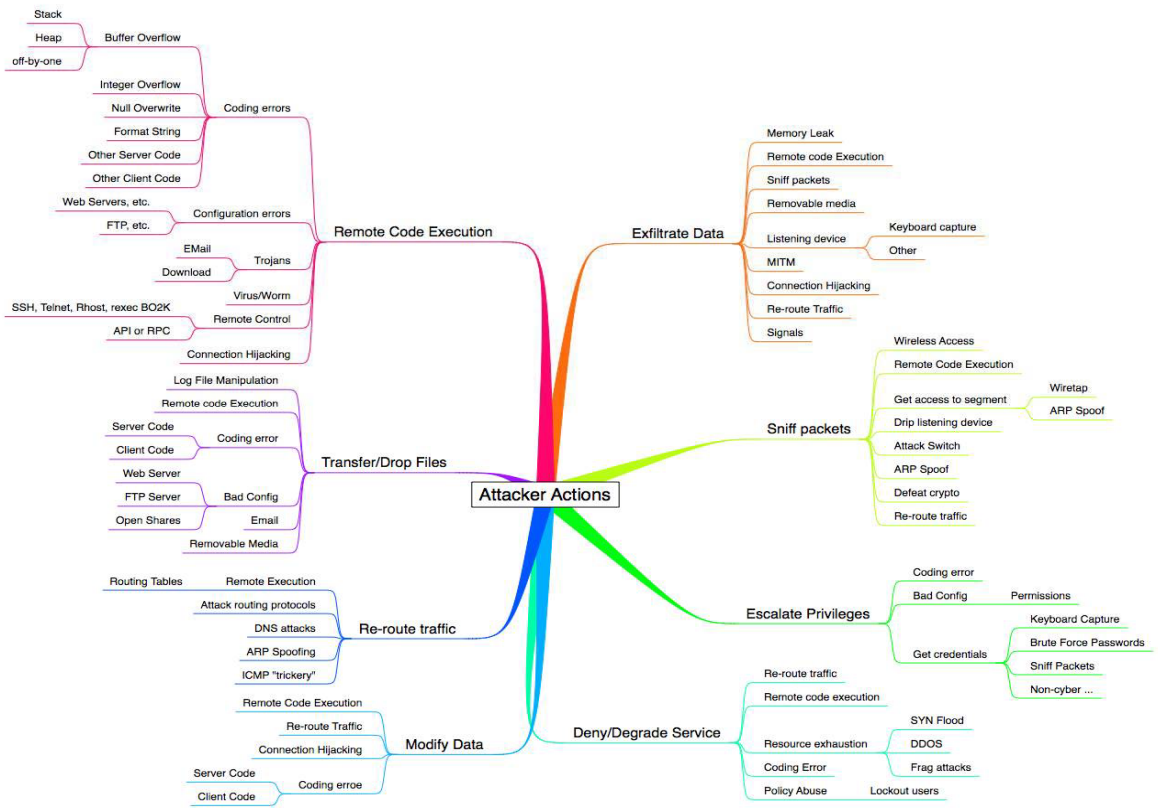

Figure 10 - Attacker Action Categorization Development

A priori methods will detect novel or novel variations of cyber attacks and rely on high value or overlapping observables. Some of these observables will be overlapping between high-value targets, hopefully allowing the analyst to develop a fewer number of unique observables, making observable generation easier. Finally, a priori characterization of the adversary can help reduce post-attack investigative effort and duration by reducing the number of potential avenues for inquiry on a computer network.

Dr. Golden G. Richard III , "Breaking the Performance Wall: The Case for Distributed Digital Forensics"

Mr. Richard pointed out the performance limitations of existing single-CPU forensic workstations and presented a cluster approach to forensic examination that significantly increases the speed of data retrieval and searching. CPU speed, memory size, and fixed-drive access speed

restrict the scope and timeliness of ‘right-away’ forensic analyses. Preprocessing techniques that establish keyword indices, image thumbnails, etc. require up-front delays on the order of days. Neither of these methods are responsive to ‘quick-look’ requirements of today’s forensic examiner.

In addition to the routine types of searches performed by examiners, Dr. Richard presented a list of other capabilities that could be helpful in a forensic investigation, to include:

- Synopses of digital files (extraction of key frames)
- Automatic feature extraction and analysis of images
- Automatic stego detection
- Voiceprint identification in audio files
- Generation of searchable text from audio files
- Background digital evidence processing during preprocessing
- Timely, live regular expression searching on large media

A means to achieving these capabilities is cluster computing. This is not done currently, probably because most people think in terms of a bigger, faster single computer that costs a lot of money. Also, most forensics tools are not designed for a clustered environment, so someone would have to write the software. However, extensibility of a clustered environment to permit execution of existing sequential forensics tools (e.g. stegodetect, hashing, etc.) would be highly desirable.

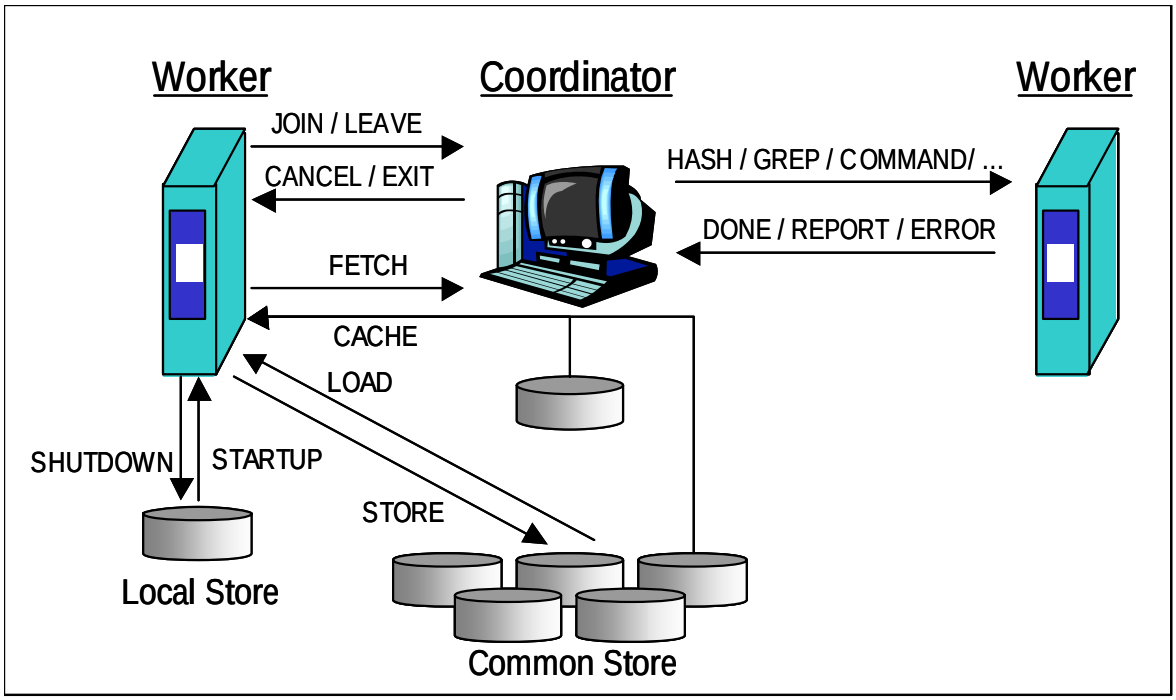

Figure 11 - Distributed Digital Forensics (DDF) Architecture

Using N-clustered computers, a greater than N-fold increase in performance can be achieved because the tasks are distributed and more of the tasking can be performed in RAM instead of via hard disk. When coupled with RAIDed storage media, loading the file server for the cluster can occur even faster, reducing the loading bottleneck. With more nodes comes higher probability of failure of at least one component, so graceful fail-over capabilities are required to reduce impact. Dr. Richard also developed a protocol to enable cluster noeds to join, leave, fetch and store files, report errors and progress, and to perform commonly-used functions such as crack passwords and create image thumbnails.

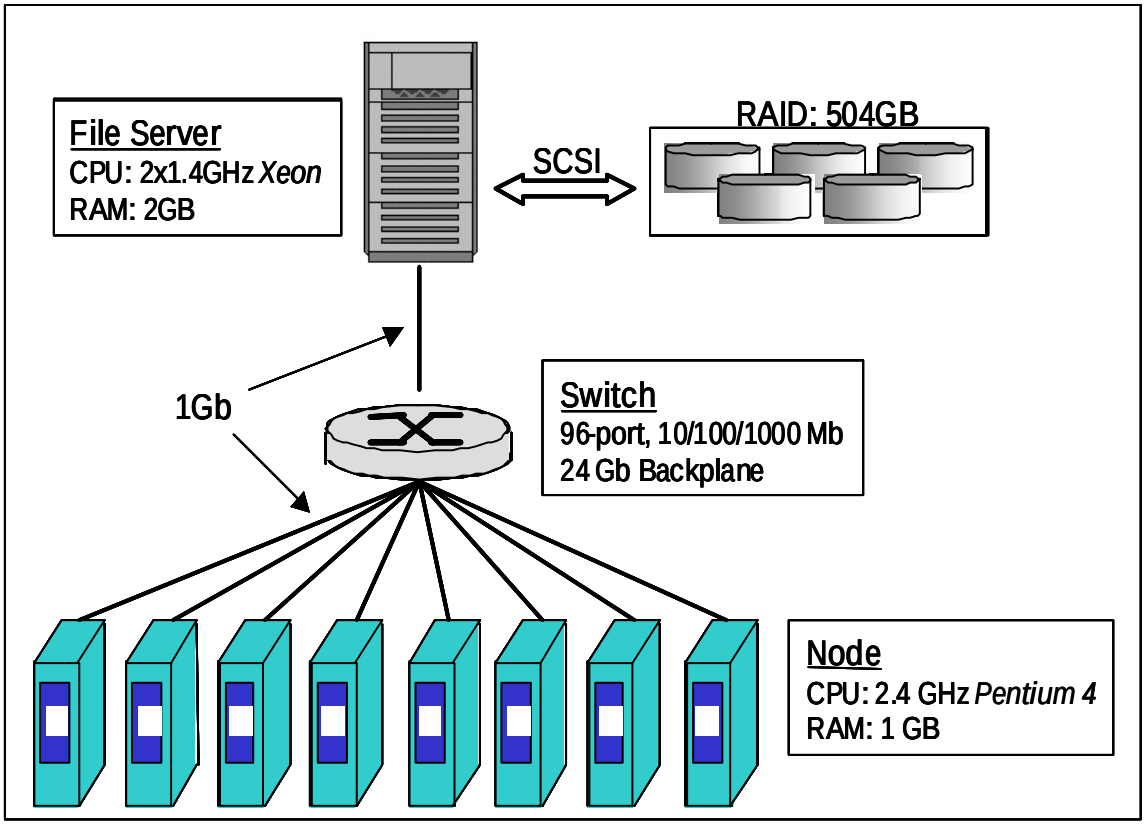

Figure 12 - Experimental 8-Node Cluster

A performance comparison between a single high-performance forensic analysis workstation and the 8-computer experimental cluster yielded a 20% improvement in loading the fileserver with files to be analyzed. Stego detection also exemplified a marked improvement in performance, shortening the time to analyze a 6GB image by a factor of 9.6. Live and regular string search time was also reduced, by a factor of 16 for a live search and a factor of 83 for the regular search. Note that these reductions are greater than the multiplicative factor of 8 nodes.

More improvements have been identified for this distributed cluster, including improving the visual interface and fault tolerance, cleaning up code, and developing intelligent caching schemes to support larger images.

Panel Discussion

To initiate debate, a panel discussion was held with four experienced individuals representing R&D in government, private sector, and law enforcement.

- Mr. Phil Turner, Technical Manager, Digital Investigation Services, QinetiQ, UK
- Mr. James Collins, AFIWC, Defensive Counter Information Division
- Dr. Frank Adelstein, Senior Principal Scientist, ATC-NYCorp
- Mr. John Ward, Senior S/W Engineer, IDEAL Technology Corp.

Editor's Note: Four questions were developed for this discussion, however, only Questions 1a and 1b were posed, due to time limitations.

Forensic analysis identifies facts or high confidence metrics uncovered by the application of known, proven, and accepted methods. These facts may be used to persuade or influence decisions across investigative domains.

Question 1a: What do you see as the greatest challenge to the use and/or admissibility of forensic evidence collected in near-real-time or in-time environments?

ADELSTEIN: Analyzing live running systems and dealing with moving targets where things change. In some cases you have no choice but to address the live system, because the system is too critical and you can't take the system down. So you have to get the data off of the running system, or you don't get any data at all. When you capture data off a live system, your frequently can't go back to the 'original data', since it was only a snapshot and it changed over time. Being able to create and understand that this is a snap shot is the biggest challenge. As an analogy, photos of evidence – physical analysis – that describes what is there at a given point in time. Later when you go back, the body isn't there. There should be some similar concept for the digital realm when capturing the information as a snapshot.

WARD: What is real time? Time is compressed when performing activities in the field. 'Really fast' is relative; months, weeks, days, hours.

The challenge would be attempting same analysis performed now, to get quick turn-around results. Try to think of a good turn around. Another challenge is collection in the field from a remote site.
TURNER: Speed in which the investigator makes the decisions. May be the wrong decision but later you will need to justify that. The decision needs to made to capture the evidence quickly, as the results of decisions are survive or sink.

COLLINS: Our operational point of view in the Air Force uses the Triangle module. Top levels (of reporting and management) will get information from bottom levels. Info feeds up through the hierarchy of command. It's a complicated system that takes different feeds and correlates them. The information that gets sent up are real time alerts. When we see an event occur, we know the exploit, and then we ask for additional information, depending on the person doing analysis. However, we run the risk that after a while, the storage disk that captures this information will write over information, and the original data will be gone. How long can it maintain the data in the database? We also have issues with timing as far as putting together the real time alert (e.g. may not really be real-time, but several minutes afterward, or later.)

Question 1b: Does the greatest risk to investigative credibility come from what you do or do not include in your real-time analysis?

ADELSTEIN: How do you best preserve the pertinent evidence? Who has access to the evidence? How do you know you can trust what you got off the computer? How do you know that was all of the memory that was in the system? Then apply the best practices. We are still early in dealing with data in motion. Practitioners are still hesitant to use this approach. The challenge is how to show what is changing over time. We could use hashing – a memory dump of an executable – where some pieces are changing. But the bulk of the system still hasn't changed. You are left with time variations, but not an exact answer.

TURNER: We are not sure what the entire digital environment looks like. We can bag stuff on the fly and tag it, but what that container should look like we don't have a clue yet. If you can solve what that bag

looks like then maybe we can do real time analysis easily. Perhaps an image file format – extensible to capturing all of the hard drive or some part of the hard drive. Maybe that universal format could be modified in certain ways. Maybe if the bags of evidence were smaller it would help. Need to come up with a digital bag as a way of capturing the data.

How do I capture this evidence and preserve it? Take a leap and see the future where the volumes are so huge. Also, we need something to indicate confidence in our analysis. But we can approximate this and have confidence that it is in a valid (accepted) range? There is something we are missing to show confidence.

Workshop Sessions – In-Time Forensics

The remainder of Day 2 was devoted to concentrated workshop discussions. The workshop topics were chosen to stimulate dialog about concepts, challenges, and technologies relating to time in digital investigations. In addition, the question was posed to one group – "Can the frameworks discussed in Day 1 withstand the strain created by time pressures in an investigation?" The following list summarizes the categories and topics addressed in each workshop:

- Time & Performance
- In-Time Forensic Technology
- Time, Accuracy, Integrity
- Framework & In-Time

In addition to expected dialog, the group discussions uncovered new, unanticipated challenges as well as potential approaches to problem solving. However, the groups focused primarily on the following foundational issues regarding in-time forensics:

- How will timeliness drive performance requirements?
- What are the future technology enablers and disruptors?
- Can we establish metrics for timeliness, accuracy, or integrity?
- Does digital forensics constitute a paradigm shift from other forensic investigative disciplines?

Group 1 – Time and Performance

> ***"Time and Performance are related issues when applying forensic methods in operational environments. A spectrum of scenario-dependent frameworks must exist in order to meet the appropriate balance for a given investigation"***

Topics to be Addressed:

It is proposed that criteria for time requirements associated with evidence discovery be developed, that could be used in various investigative environments. Consider the different criteria that would be required for prosecution, business, military, and intelligence applications, among others. Do subgroups apply? Would criteria be different for transaction processing, logistics, support systems, civil, criminal, etc. within a particular application domain? In addition, it seems evident that analysis performance enhancements will be requited to meet new time constraints. Group these enhancements according to technology area, and comment on what is available, conceptual, and the spaces in-between. The impact your findings will have on the Framework concepts we have been discussing

Group Leads

Facilitator: Dr. Golden Richard III, Univ. of New Orleans
Recorder: Eric Ozanam, AFRL/Northrop Grumman

Group Focus

Two major factors come into play when dealing with In-Time Forensics. Time plays a pivotal role in regards to "in-time forensics" since the speed by which investigation can proceed is governed by the time it takes to assemble relevant evidence. The subsequent issues related to in-time forensics are the necessary "performance enhancements" to meet the new time constraints that are dictated by various operational environments (domains). The theories discussed here are pertinent to the discussion of various frameworks, and are noted here.

Overview of Group Deliberations

The general consensus of this group[6] and the topics discussed was that, regardless of the domain, "time and evidentiary discovery" hinged on four major factors:

- Investigation time and financial resources.
- Methods of data reduction.
- The differences between legal requirements of forensic evidence, and evidence that can be accepted as "good enough".
- A learning curve exists across domains that demonstrate a discontinuity among methodologies, best practices, and policies.

To achieve adequate means of performance the group decided that it is necessary to address "time requirements" across the various investigative domains. The group felt that five forensic technology areas would need to be addressed or enhanced to achieve adequate performance metrics, which included:

1) Better data reduction methods.
    - Block hashing
    - Bloom filters
    - Better (new) algorithms for file identification
    - Better drive imaging technology
2) Better visualization tools.
3) Instant access to evidence.
    - Threaded applications (e.g., don't make me wait for thumbnail generation)
    - Background evidence pre-processing
4) Smarter imaging methods.
    - Don't even image e.g., system files
5) The ability to conduct "live analysis" or "in time" forensics
    - A quick peek: e.g., Mobile Forensics Toolkit

Concluding Decisions

[6] Participants were Barya Baryamureeba, Cheryl Brown, Ian Bryant, Marty Gray, Natalie Harrison, Jordan Jacobs, Brian Kropa, Larry Leibrock, Jim Lyle, Ava Martin, Jim McIntyre, Eric Ozanam, Nikita Proskourine, John Tebutt, Doug White, and Ren Wie

The major themes that rose from our discussion seemed to focus around the idea that there is a significant variance when an analyst seeks out “forensic evidence”. The group clearly identified instances in which “proof” or “suggestion” was valid or invalid according to investigative environments or situational needs. For example:

- Time Critical: Good and quick enough to make a decision
    - Airplane vs. Ship vs. Train vs. Car vs. Pedestrian
- Corporate/University: good enough not to be sued, and no image tarnishing
    - Breach of Policy
    - Civil Legal Action vs. Disciplinary Action
    - Internal vs. External leakage
- Criminal: Reasonable doubt, decision of Jury
    - Minor Offense
    - Major Offense

The group decided that a spectrum of frameworks must exist in order to select the proper course of action. These frameworks should be “scenario dependent”, and relax or tighten its requirements seamlessly.

Group 2 – Technologies/Research and Development

> ***"Pre-incident preparation [a new process step] may ultimately be the greatest enabler for in-time/real-time forensic technology and response."***

Topics to be Addressed:

After-the-Fact methods may map partially to In-Time Forensics, but new techniques will be necessary. Present current digital forensic methods may be adaptable in whole or in part. Consider any functional limitations that would accompany the transition to the practitioner. Discuss emerging areas in R&D that may affect adaptability of digital forensics to the mission space - consider two perspectives; Technology that makes digital forensics more difficult or time consuming, and; Technology that enables digital forensics (i.e. improving process) Will any of these technologies require changes to the existing practitioner skill sets?

Group Leads

Facilitator: Chet Maciag, AFRL
Recorder: Nelson Lee, AFRL

Group Focus

This group attacked these questions by first considering the current role of framework and process in digital investigations. After spending some time on that topic, the group proceeded to enumerate the key conceptual challenges to achieving in-time forensic analysis. From there, a list of technologies was assembled that are currently serving to hinder or slow down the analysis process. Finally, the group also devised a list of potentially promising technologies that could serve to speed up the way forensic investigation is currently performed.

Overview of Group Deliberations

Adjustments to the Framework

The main idea stemming this discussion is how to handle deployment of tools for a real-time/in-time investigation. The current model of thinking follows these steps: Preservation, Collection, Examination,

Analysis, and then Documentation. We will need to change this process to Preparation, Collection, Examination, Analysis, and then Presentation. In the new Preparation phase, forethought is given to the potential avenues that might be exploited by an adversary to compromise an information system. Those avenues serve to influence the placement of surveillance and incident response tools on a computer of network. The Preparation phase is also the time in which first-responders are trained on how to detect and respond to digital threats in a timely manner. Completion of this crucial first step can serve to effectively reduce initial reaction time and provide key indicators on how to pursue a digital investigation before the trail goes cold.

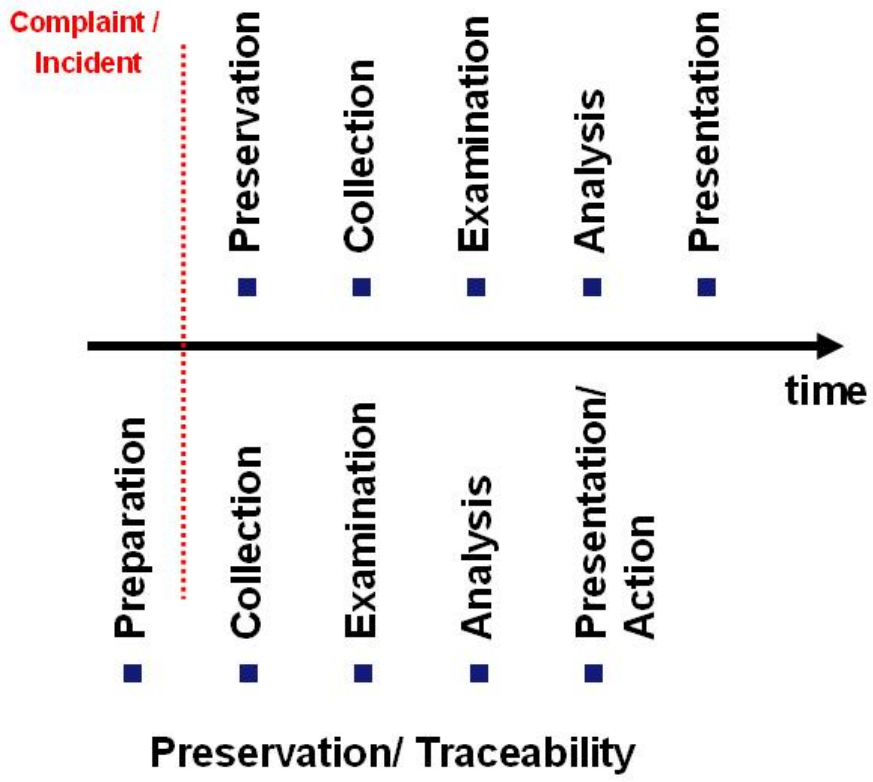

Figure 13 - Addition of a "Preparation" Phase to the Investigation Process

The group noted that preservation of evidence, and traceability of how evidence is processed, handled, and analyzed, were integral facets of each step of the process. As a result, Preservation/Traceability was drawn out from an explicit process step, and indicated that it was part of each step of the process.

Key Conceptual Challenges to In-Time Forensics

Challenges for in-time forensics:

- Adaptive models - The need to deal with unknown scenarios in a valid and confident sequence of steps
- Layered, interconnected, complex systems
- Meta-evidence – what needs to be gathered from a live system to be used as admissible evidence?
- Evidence priority must change - RAM disk vs. hard disk
- Snapshots – Taking the snapshot of a live and/or distributed system and/or analysis of successive snapshots
- When do we know data capture is complete?
- How can we have traceability?
- Up to what point can you trust the evidence that you are collecting on a live machine in real-time?
    - One approach mentioned was to take continuous snapshots of the data and when an intrusion occurs, you stop trusting the data from that point on.
- How can we handle deployment of a real-time investigation?
    - Pre-load the forensics tools on the system when the computer is staged in the IT department.
    - The investigator brings the tools along in their toolkit, and does the best they can during an on-scene investigation.

Hindering Technologies

The group developed a list of some of the technologies and factors that will negatively impact forensic timeliness:

- Embedded encryption at the hardware level now posses a problem during analysis.
- Hard drive space is now becoming an issue since the average computer will now have several hundred gigabytes. We will need the equivalent amount of space to image the drive and perform analysis.

- Distributed systems are increasing in popularity. Investigators will need to broaden their knowledge set to include network forensics. New challenges in this area include attribution of actions in peer-to-peer (e.g. file sharing) systems.
- Anonymizers and anonymous systems (e.g. email) are becoming wide-spread and will add complexity to the analysis.
- Evolving technology that needs to be considered:
    - New forms of communications such as IP telephony
    - Multiple layers of independent technology
        - E.g. Data services that ride over mobile telephony.
    - Traceability of ad-hoc/prepaid networks
    - Quantum communication networks
        - In theory, all wiretapping is detectable

Enablers of Forensics

The group outlined key areas that would enable the forensic investigator to be more efficient at completing tasks In-time. The following list outlines some key discussion topics:

- Paths to bypass means of encryption to capture raw data, for example, system bus-level tools
- An expanding/extensible toolset - “The right tool is needed for the right job.” The tools that investigators are bringing to the crime scene are becoming outdated. Further research must be needed to keep the investigator ahead of the criminal.
- Tools with the ability to perform analysis on large volumes of network traffic data
    - Distinguishing between system level vs. host level
    - Correlations
    - Understanding violations of policy, indications, and warnings
- Quantum Computing holds the promise of breaking complex crypto key lengths that currently inhibit pre-attack monitoring or post-attack decryption of covert communications.

Another issue that needs to be addressed is the core competency of the investigator. The question raised was, “What does a person (who has low

competency) need to do when they approach a computer that needs in-time forensics?” One solution is to present an adaptive framework, which can deal with unknown scenarios such as In-time forensics. The investigator can then be confident in following a series of outlined steps.

Concluding Decisions

A requisite “Preparation” phase will need to be added to current investigation models, in order to most effectively leverage latest technology, avoid the pitfalls of disruptive technology, and to ensure that data collected “in-time” is actually usable for “in-time” investigations. Otherwise, lack of preparation will lead to incomplete or inconclusive information, and effectively blind-side the investigator after it is already too late.

Group 3 – Time, Accuracy, and Integrity

> ***Time, Accuracy, and Integrity: "The combination of these 3 elements defines a function that details the usefulness of digital forensics in a near-real-time investigation."***

Topics to be Addressed:

The combination of Time, Accuracy, and Integrity define a function that details the usefulness of digital forensics in a near-real-time investigation. There are trade-offs between the capabilities that require consideration for each investigation. How do these elements relate to each other so the function best supports decision-making across investigative domains? In addressing this question, consider the use of evidence in a spectrum ranging from operational action (decisions assigning resources to problem areas) to prosecution. Will this have any practical impacts to the model we have been considering? How will the Framework be impacted (e.g. Does our framework adequately accommodate 'time' criticality? What metrics are needed to really discuss accuracy?) Finally, will the spectrum of "Who can collect evidence" be expanded? For example, sworn examiners can't be everywhere. Who can be trusted to provide probative information? Is there a spectrum of "acceptable integrity"?

Group 3A Leads

Facilitator: Jack Mineo, AFRL/MIN

Recorders: Mark Williams, AFRL, Laura Wood, AFRL/Booz Allen Hamilton

Group Focus

The main focus of this group[7] was to decide what exactly Time, Accuracy, and Integrity really defined. The discussion furthered on to how the three elements would impact the framework and how to leverage time and technology employing the iterative process. Furthermore, this group discussed who could collect evidence for probative value.

[7] Participants were Jack Mineo, Frank Adelstein, Laura Wood, Dwayne Allain, Bernie Cowens, Fava, Thomas Marenic, Eoghan Casey, Rob Joyce, Mark Pollitt, Lance Spitzzner, Sam VanMeter, Brian Carrier, Jim Christy, J Jones, and Mark Williams

Overview of Group Deliberations

The group facilitator Jack Mineo started the discussion by giving a brief overview of the first question and his thoughts on the interaction of time, accuracy, and integrity. Jack discussed the need to consider as many domains as possible when exploring the key measures and relationships between these properties. He initiated the discussion by drawing a timeline with court cases on the left and military reaction on the right.

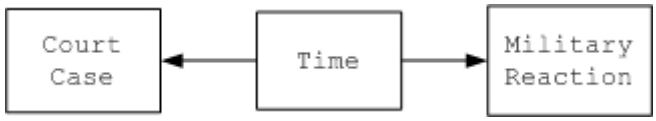

Figure 14 - Continuum of Requirements for Timeliness of Digital Investigations

It was determined that the earlier one gets an indicator of what the evidence will be used for, the better the answer will be in determining how one captures the data. Jack commented on the value of the data and the importance of time in relation to that data. Also mentioned was that if the data is about a kinetic attack, the timeliness and then accuracy of the information are more important than the integrity. Mark Pollitt contributed to the discussion by pointing out that the accuracy and integrity of evidence are on the same plane and that the value of accuracy and integrity are not fundamentally different

In the context of the above Figure, Jack said that time is less important in a court case while quality is more important, yet in the military, quality and time are both important. Although evidence must be seized quickly in a criminal or civil matter, time is generally spent preserving evidence and a failure leading to an incorrect verdict is unacceptable. Conversely, in a military situation, the reaction time may need to be instantaneous to save lives and a false alarm is acceptable. To further Jack’s discussion he talked about the automatic computing system administration function, that automating systems would make it easier for the system administrators to be able to spend their time doing human functions while the computer does what it is good at, which is automating processes.

Eoghan Casey mentioned that automated response and audit logs depend on the trust of the system process and these processes can be undermined when the underlying system is compromised or error prone. Underlying trust is critical and yet hard to determine. If the value depends on the need for a legal measure then the validity and integrity are crucial. If there is a commercial need, dollars and cents are critical. As for military, time is critical.

The group decided they needed to define what the three elements meant:

- Accuracy – the correct representation of what is being viewed. How 'right' is the information?
- Integrity – the degree in which you can rely on the information
- Time – when the information is needed
- Trust – accuracy and integrity
- Value – the significance of the information in the given context

Metrics can be developed from these definitions and the relationships between these properties in a given context.

Concluding Decisions

The result of the discussion was that the value of the information was determined by the application and/or need with time as the primary issue. The value of the information balanced with the time factor will determine the process that will be used. Therefore, choose a process that provides the highest trust within the time constraints. As far as the impact of time, accuracy, and integrity on the framework, this group decided that trust in the accuracy over time requires integrity. Lastly, the question on who could collect evidence, the group decided that anyone should be able to collect evidence, not just law enforcement. However, the information that is collected has to be of value and have demonstrative trust commensurate with the environment/situation within which it is used.

Group 3B Leads

Facilitator: Heather Dussault, SUNY Institute of Technology

Recorders: Nicole Beebe, Univ. of Texas at San Antonio, Tanya Allen, AFRL

Group Focus

The main focus of this break-out group[8] was how the three elements; Time, Accuracy, and Integrity related to in near-real-time investigation. The most part of this group's discussion was deciding what time, accuracy, and integrity really meant in relation to digital forensics and furthermore, what the exact definition of the three elements is. The discussion also led to how the three elements related to one another.

Overview of Group Deliberations

The group decided that the definitions were as follows:

- Time: If you hurry, you can't get the best job done. Improvement needed as far as time for collection. Many factors involved when considering time.
- Accuracy: Of the data initially. Do we have to sacrifice accuracy? As a question of time – immediate accuracy is needed. The effects of accuracy are: life, health, public safety. The trade off is that it may not hold up in court.
- Integrity: The exact data is the right data.

Many questions arose during this group's discussion in which some were answered more than others. Some example questions include:

- Do we lose accuracy if we do things quickly?
- Can we have more efficient algorithms to do things faster?
    - Hardware advances, better software, better algorithms
    - For the most part a human will always be involved
- Is integrity the process where you confirm your accuracy?

[8] Participants were Heather Dussault, Nicole Beebe, Tanya Allen, Kyle Dempsey, Brian Croniser, Jim Collins, Mike Duren, Yong Guan, Matthew Kucenski, Bob Pasquarella, Gary Price, Chris Sanft, Kulesh Shanmugasundaram, Phil Turner, Florence Tushabe, Geoff Weidner, and Christopher Williams

    - Integrity – doing the best job with the tools you have available at the time.
    - Integrity = Trust
- Do we take the time or not?
    - No – need faster machines
    - Yes – machines are good plus human ability

The group spent most of their time discussing the three elements. However, they also discussed the process as far as the three elements effecting the framework (if one at all). The group came to the conclusion that the framework phases will be the same but what/how you achieve the goals of the framework will be dependable. As the framework relates to the three elements, accuracy and integrity will have different roles depending on the situation and time will be relative in anything you do. What the group decided is the best but may not be practical is to have high accuracy and high integrity while limiting time to none.

The rest of the group's discussion dealt with who can collect evidence to be expanded? Questions brought up in this section included:

- Remote Forensics?
- Everyone interprets data in a different way – so do people corrupt the data then?
- Everyone in civil until handed over to the police?

The group decided that humans still have to run the machines. There are still the issues as far as humans needing guidance, human intelligence (better way?), and the thinking process of different human beings.

Concluding Decisions

The group decided overall that humans will still need to be involved in the investigation process for the most part. We need human intelligence along with machine capabilities to do the best job we can. The group concluded that we want to be able to capture data and then react in real time without having any fallacies as much as possible. This group wanted to have a framework that provides us with high

accuracy, high integrity and no time. This may be to simplistic of an idea and it is too complex to tackle. For right now the group decided that Brian Carrier’s model included time (event) issues; state changes; and cause-effect. This would be a start or the best framework for now and it could be adjusted to fit everyone’s needs depending on the situation.

Group 4 – Framework and In-Time

> ***"The Digital Forensic Framework is viewed mostly in the realm of traditional forensic investigations. There is no fundamental paradigm shift in how we treat digital investigations over traditional ones."***

Topics to be Addressed:

Our discussions so far have viewed the Digital Forensic Framework mostly in the realm of traditional forensic investigations. [However, we need to consider how that investigative model will need to evolve to meet future technology and timeliness requirements. - Ed.] The group is to discuss how this paradigm shift from more traditional search-and-seizure or brick-and-mortar crime labs, to the virtual or live crime scene, impact the field as a whole? In addressing this question, the group should consider how will this shift impact the models for the Digital Forensic Framework we have been discussing? In addition, suggest or recommend a path to adapt some of the major difference in this new paradigm to the Framework and Digital Forensics as it is currently practiced.

Group Leads

Facilitator: Chet Hosmer, WetStone Technologies, Inc.
Recorders: Scott Rey and Thomas Parisi, AFRL

Group Focus

The group[9] focused on whether a paradigm shift from a physical crime scene to a live or virtual crime scene will impact the field of forensics and the framework.

Overview of Group Deliberations

The initial discussion was based upon Sarbanes Oxley and the fact that whoever destroys or tampers with records will be subjected to the most severe sanctions. The group then addressed the issue of a timely

[9] Participants were Chet Hosmer, Dario Forte, Chauhan, Lorenzo Martignoni, Kelsey Rider, Todd Shipley, Art Conklin, Mark Hirsh, Jack Lewis, Scott Rey, Gary Palmer, Lang, Justin Levinson, Paul Blythe, Will Platnick, Thomas Parisi, and Pete Ware.

investigation where they determined that “timely” is dictated by circumstance.

In any circumstance, there is always a need to image a hard drive. However, the problem arises where resources may not be available and only a portion of the hard drive may be captured. A real-world scenario was given for comparison. If a murder occurred at a hotel, the investigators would tape off the area of significance. They would not need to seal off the entire hotel. In comparison to the capture of digital evidence, we need to determine what of significant value is on the hard drive and only capture that portion.

On the lines of admissible digital evidence, the group mentioned the point that the prosecutor must present the best evidence at hand, but not all the evidence. It will be up to the defense attorneys to cross examine and refute the validity of the evidence.

Concluding Decisions

The conclusion of the group is that the term “forensics”, from a Law Enforcement point of view, only applies to “evidence”. The term “evidence” only applies to material that is intended to be used in court. One example presented was: A military operation for purposes other than the prosecution of criminals, are not “forensics”. People use the term “forensics” inappropriately because it is an attractive word.

The group also decided that there is no paradigm shift. Digital investigations require different technological tools to collect, analyze, and present evidence, but the fundamental process of how investigations are performed is not “revolutionary.” All is required is careful modifications to current processes.

Lastly, the group also decided that there is no vehicle between Military, Law Enforcement, Academia, and the Private Sector to define problems and assign groups to solve them. [Apparently groups such as IASIS, HTCIA, IEEE, TSWG, etc. are not cross-cutting enough, nor have a broad enough charter to engage and bring consensus among all the relevant players.]

Day 3 – Special Topics in Digital Investigation

Introduction

Inevitably, every conference or workshop receives more good papers than it has time for in its schedule. Or, the papers are so intriguing or informative that you simply cannot turn them away. Day 3 was not different. The DFRWS paper committee received a number of papers that did not fit squarely into the themes of Framework or In-Time Forensics, but represented topics that were of significant value to the DFRWS community. Accordingly, the following three papers were presented and are summarized in the following pages.

Plenary Speakers

Ian Bryant, "Forensics for Critical Infrastructure Protection (CIP)"

Mr. Bryant discussed the complex CIP environment (in an United Kingdom context), and the challenges in defending and sharing information for mutual defense. He also detailed the complex relationship between cyber and kinetic domains, and the variety of interested parties that should (but don't always) coordinate to protect the cyber infrastructure, despite their interdependence on common infrastructures. The biggest challenge is timely and effective triage of cyber attacks between these parties, without accidental contamination of cyber evidence during the detection and investigation process.

In summary, there is a widespread need for forensic services in information assurance. A triage process is essential to determine speed, scope, and purpose when forensic involvement required. Forensics activity must not become a denial of service (DOS) itself. The biggest challenge to Forensics is outside the control of its own community, particularly when it pertains to the prevention of evidential contamination during detection or triage.

Mark Hirsh, "Formalizing Forensic Test and Evaluation Activities”

Mr. Hirsh’s talk covered the rationale for conducting test and evaluation (T&E), the DoD Cyber Crime Institute’s T&E process and procedures, DCCI’s findings, and the rationale for creating a centralized repository of T&E results.

Both the forensic tool user and developer benefit from T&E. The user reduces the risk of surprises in tool function, performance, or reliability during use. The developer can use T&E results to help influence future market decisions and identify areas of tool improvement. T&E can be either user- or customer-driven. Not all tools perform as advertised or expected the first time through testing, or are dependent upon a specific platform or hardware suite. A successful test, on the other hand, does not guarantee a product will necessarily work or will be reliable, since exhaustive testing isn’t possible.

There is currently quite a demand for T&E. DCCI cannot satisfy all requirements, and is looking for partnerships with other test organizations. Some testing gets performed redundantly because there isn’t good sharing of test report information between testing organizations. There needs to be a central repository for test reports, and the reports need to be developed in such a way that tests are repeatable, understandable, and easy to interpret. Parting recommendations by Hirsh included the establishment of a testing ‘message board’, to help communicate test activities and results to related communities of interest.

Michael Sieffert, "Stego Intrusion Detection System”

Mr Sieffert described the current threat environment, and potential for the use of steganography on the Internet as well as the corporate environment. Steganography is an enabler of covert communication, which can be used by adversaries to use your networks for long periods of time without being detected. One such adversarial information exfiltration method might embed sensitive corporate information in

company web page images, and then the images are plainly downloaded from the company website without challenge. The stego intrusion detection system is a network device that targets HTTP traffic, analyzing web page images for embedded information and covert communications.

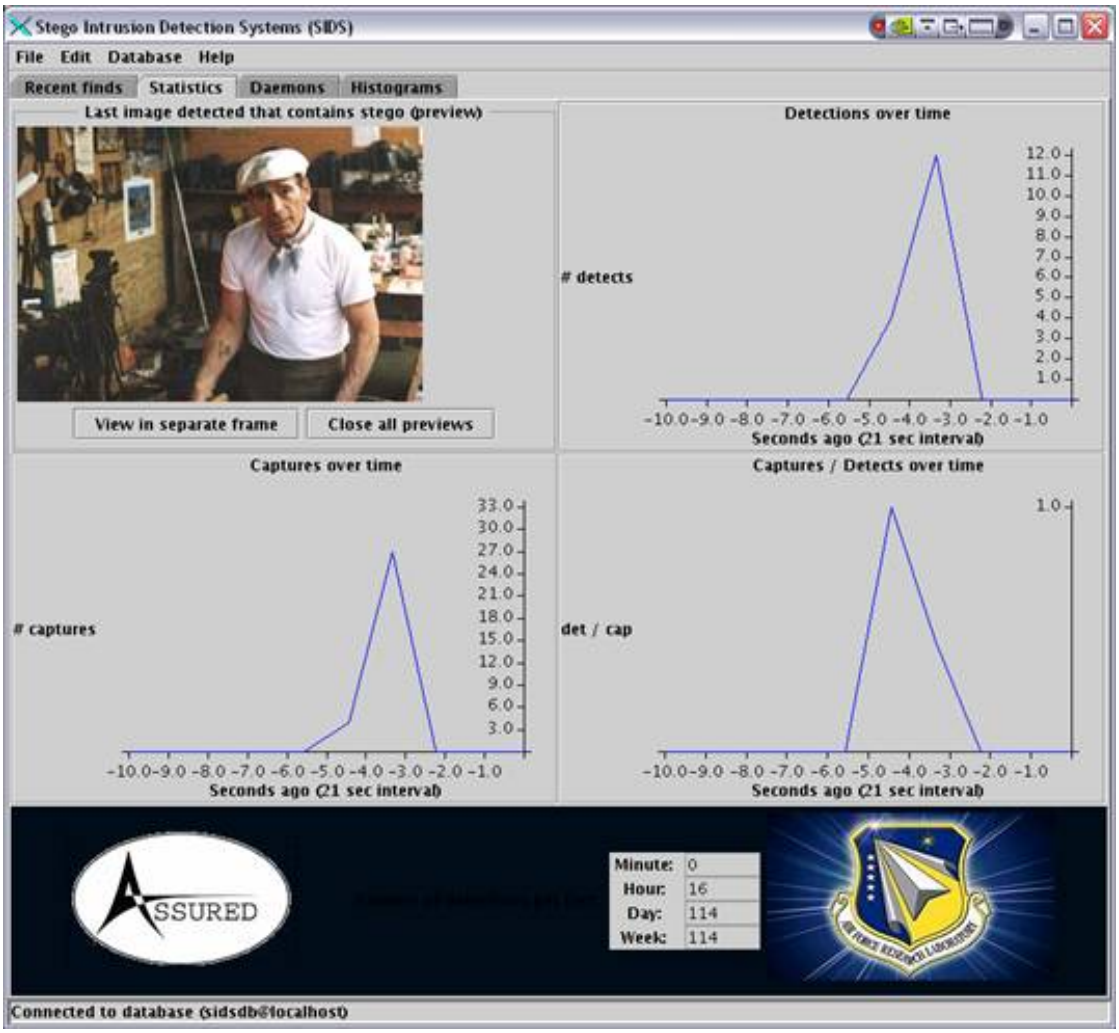

Figure 15 - SIDS GUI and Statistical Analysis

There are always limitations to cutting edge capabilities, and SIDS is no different. Extremely high traffic can cause data loss. Although SIDS is modularly expandable for other stego algorithms, only a few are currently supported. And, encrypted data still cannot be examined. A host-based version of SIDS is being pursued in the future.

Day 3 Ending Suggestions for Future DFRWS Workshops

[Ed. - Paraphrased from attendees' comments]

1. **Eoghan Casey**: Applying the Framework models?
    - **Possible Task**: It would be interesting to discuss how each of the DF Framework models we saw this year applies to or in various investigative domains. Examples of domains of interest are:
        i. Courts/Legal/Law Enforcement
        ii. Defense/Military/Intelligence Community
        iii. Corporate/Business/Transaction Processing/Policy Enforcement

    - **Comments**: We think that these seeding the List Srvr and Forum with this type of discussion may be fruitful but it has to be handled carefully. Throwing a statement out there worded like the first bullet wouldn't be very meaningful or useful to a participant that had not attended the workshop or read the material before hand. We would preface the seeded message with an invitation to read the material posted on our web site so that all the folks involved will be "on the same page" for the dialog/debate to follow.

2. **Brian Carrier**: Who is using the List Srvr?
    - **Possible Task**: Brian asked a question about the demographic breakdown of the List Srvr membership.
    - **Comments**: To our knowledge we don't have that information and We are not sure that we can actually get at it to report back with an answer. This is the case because it is a very "open" list. Short of the requirement to have an email address, there is absolutely no vetting that takes place before an individual can participate. So all we have to make the kind of assessment that Brian asked for is the email address that we are given to use. Besides issues of trust related to that address and the possibility of using anonymous mailers or mass mailers, the domain information provided in the address has

limited use unless a more detailed assessment were undertaken. By this we mean using whois , tracert (traceroute), and manual means to gather additional information. We are not sure we have the resources to do this or that we even want to. Individual participation in various discussion and associating emails with those folks we already know may lead to really getting to know persons but short of that it is a very non descript service that we have set up

3. **Suggestions for Mini-Workshop Themes** (or virtual discussions as well):
    - **Large Data Sets**: This issue looms above other advances made in our field. Especially in the LE domain where the current edict dictates that everything must be examined (exculpatory potential). It certainly deserves a closer look. There may be real tie in with work like Golden has done related to improving performance, employing clustering technology, and analysis using memory cache.
    - **Digital Forensic Triage**: This is an especially pertinent issue for the LE first responder community, but also very important in the I&W, CNO space (mission operations) where timely situation assessment is paramount. Certainly based on the very good work we saw from Ian Bryant (NICSS , UK) we can jump to more detail at a rapid pace. We also see Honeynets, and John Lowry's work as major sources of input on this topic.
    - **Decision Quality Information**: Information fed to all decision makers whether in courts or not must be factual and persuasive. Persuasiveness is effected in some part by the metrics or confidence associated with that data. To some degree this topic may help to counteract the negative effect of Large Data Sets or constantly growing densities. If the community can research discover and agree that certain information, if available, is sufficient to make a case or proves a point with high confidence then that will be a step in the right direction.
    - **Intelligent Collection** (Phil Turner's specialty or area of keen interest – he could be a strong focal point for discussion on this topic)

- **Relation of Speed and Completeness in Forensic Analysis**: Going with the premise that forensic analysis, methods and techniques, can be applied outside the pure LE space what are the particular criteria that make sense to use? Some investigative areas that may be interesting are:
    i. Intel – if the right folks can participate (true for al though)
    ii. Military – Depot, theater, logistics, NOC, etc
    iii. Commercial, Corporate, Finance, e-business, ISP, etc
- **Data Hiding (DH)**: Stego detection and extraction are all the rage, but as was pointed out by attendees and also at the 1st DFRWS by Spaf, Stego is but a portion of the superset of potential ways to hide data electronically. Some possible sub topics in this area include:
    i. Building a taxonomy for DH
    ii. Categorize types by technique, bandwidth, necessary experience, difficulty, etc
    iii. Building experiments to demo capability and potential for harm
    iv. Discuss techniques for identifying, capturing and preventing DH
    v. Maybe discuss how we use it as an offensive technique (questionable in an open forum)
    vi. Focused discussions in high payoff categories

4. **Getting our results used**: (general): Throughout the DFRWS we were part of several discussions (last year as well) that centered on how we can leverage successful group interaction and decision models to help us get our group concept and results recognized. The IETF and its RFC process rises to the top of the heap almost every time. This would be a great topic that, if moderated and documented properly could benefit the DFRWS's credibility and also our ability to positively influence the digital forensic community. We need to chat about the best way to implement this discussion to get community interest and to keep it moving toward a defined goal.

5. **CMM for DF Framework Models**: The CMM or Capability Maturity Model approach has been successfully implemented in System Acquisition, System Security, Software Engineering, Quality Assurance and other areas. It seems that the CMM approach may be viable related to DF Framework and DF practices in general. In general, it will be like creating a Physician's Desk Reference for DF. Some considerations are:
    - Need to make CMM material available either at DFRWS.org or provide pointers to material that folks can study
    - Need to build and present case studies of how CMM was implemented in other disciplines to learn from lessons captured
    - Need to include the Framework authors to get their valuable inputs
    - This will best move along if we involve a multi-disciplinary audience
    - Review ASCLD approach to look for comparison to CMM.
    - We need to talk more…..

6. **Metrics and techniques for DF**: Throughout DFRWS04 we heard mention that validity and practicality was in question. This is especially true for the Framework approaches. We need a concerted effort to come up with items or attributes to measure (with rigor and certainly) that will provide the most persuasive proof of an assertion (criminal or general wrongdoing) as well as an assessment of trusted (generally accepted) techniques used to collect these measurements (metrics). This is seminal and I think should be pursued early on as we proceed.

7. **Taxonomy or Lexicon for DF**: Terminology in DF is getting better but it is scattered at best. We need a consensus on the set of major definitions our field will use so that a common language can be fostered and research can proceed with mutual understanding. This could be a part of the CMM idea or another where folks think it is most applicable but it really must be done.

8. **General Suggestions and Comments on DFRWS:**

- More short talks so more talks can be accommodated and topics are more varied
- Provide a server at the conference so content may be downloaded as needed or required. This helps with efficient distribution
- Perhaps implement an “Open Mic” segment – perhaps a **Forensic Karaoke** of sorts (music?)
- Make materials available to attendees so they may have during the presentations
- Make materials available earlier – This implies we must ratchet back our due dates for many things – no more last minute stuff – better preplanning by us will be required
- Consider holding Mini-Workshops coincident with a major, topically related, conference. Helps the draw and some attendee logistics. Attendance will benefit. Should we notify the conference and let them help advertise? Lots of questions here…
- DFRWS is better served as a conference without workgroups so more presentations can be heard.
- Mini-WSs should be structures with specific tasks and assigned roles. Consider taking the time to craft case studies and ask participants to help do it before hand. They should be involved

-

APPENDIX A: DFRWS 2004 AGENDA

10-Aug-04 Tuesday

19:00-21:00 Meet and Greet Reception

11-Aug-04 Wednesday

8:00 Continental Breakfast

8:30 Welcome & Introduction

9:00 Keynote Address "A Framework for Digital Forensic Science"
Mr. Mark Pollitt Presentations Series of briefings presenting different approaches to the creation and content of a framework for digital forensics

9:45 The Enhanced Digital Investigation Process Model
Florence Tushabe Makerere University, Kampala Uganda

10:20 Mid Morning Break

10:30 A Hierarchical, Objectives-Based Framework for the Digital Investigations Process Nicole Beebe University of Texas at San Antonio

11:05 An Event-Based Digital Forensic Investigation Framework
Brian Carrier Purdue University, West Lafayette, IN

11:40 A Framework of Distributed Agent-based Network Forensics System
Ren Wei Zhongnan University of Economics and Law, China

12:15 Lunch

13:15 Panel Discussion
A panel of representatives from various domains address issues surrounding the framework and field questions from the attendees.

Panel members from:
- **Law Enforcement** - Jim Christy
- **Business sector** - Chet Hosmer
- **Forensic Training** - Chris Snaft

14:15 Workgroup Assignments Attendees assigned to groups - leaders, facilitators, recorders introduced and meeting locations designated

14:30 Workgroup Breakouts, Refreshments Available
Groups will meet, debate/discuss and document details of their particular topic area.

16:30 Workgroup Briefings
Group will brief their findings to the plenary session.

18:00 End of Day

12-Aug-04 Thursday

8:00 Continental Breakfast

8:30 Introduction Synopsis of Day 1 Activities

9:00 Keynote Address "Honeynets and Digital Forensics" Mr. Lance Spitzner
Presentations Briefings presenting concepts related to the challenge of performing near-real-time forensic in operational environments

9:45 Honeynet Data Analysis: A technique for correlating sebek and network data
Edward Balas Indiana University

10:20 Mid Morning Break

10:30 Forensics, Fighter Pilots and the OODA Loop:
The Role of Digital Forensics in Cyber Command and Control
Dr. Heather Dussault SUNY Institute of Technology & GIIT, Rome, NY

11:05 Adversary Modeling to Develop Forensic Observables
John Lowry BBN Systems

11:40 Breaking the Performance Wall: The Case for Distributed Digital Forensics
Dr. Golden G. Richard III University of New Orleans New Orleans, LA

12:15 Lunch

13:15 Panel Discussion
A panel of representatives from various domains address challenges to the adaptation of current digital forensic practice to the operational realm. What can be transitioned and used and what needs to be developed?

Panel members:
- **Corporate Forensics** - Phil Turner
- **Military LE/Counter Intel** - James Collins
- **Developers**- Dr. Frank Adelstein & Jordan Jacobs

14:15 Workgroup Assignments Attendees assigned to groups - leaders, facilitators, recorders introduced and meeting locations designated

14:30 Workgroup Breakouts, Refreshments Available
Groups will debate/discuss and document details of their particular topic area.

16:30 Workgroup Briefings
Group will brief their findings to the plenary session.

18:00 End of Day

19:00 DFRWS Dinner

21:00 **Forensic Feud** – Test your forensic knowledge from a wide variety of questions.

Forensic Rodeo - Will you find all the proof necessary to convict the suspect?

Award Ceremony - We had fun, but now someone has to take something home.

13-Aug-04 Friday

7:30	Continental Breakfast
8:00	Day 3 Intro Other Topics in Digital Forensics Presentations A series of 20-25 minute presentations on topics of interest in Digital Forensics that weren't directly related to the workshop themes.
8:15	Forensics for Critical Information Infrastructure Protection Ian Bryant National Infrastructure Security Coordination Centre, MOD/UK
8:45	Stego Intrusion Detection System AFRL/ASU Assured Information Security
9:15	Mid Morning Break
9:25	Secure Digital Camera Paul Blythe and Jessica Fridrich SUNY Binghamton, NY
9:55	Proposal to Formalize Test and Evaluation Activities within the Forensic and Law Enforcement Communities Mark Hirsh, DCCI -MITRE
10:25	How to Reuse Knowledge about Forensic Investigations Lorenzo Martignoni Universit`a degli Studi di Milano Bicocca, Italy
10:55	Brunch

11:15	Day 1 Synopsis What have we accomplished and what are our plans related to Framework.
11:45	Day 2 Synopsis What have we accomplished and what are our plans related to In-Time criteria
12:15	DFRWS 2005 Planning Discussion of next years location and possible interim meetings to discuss special topics and TEMS throughout the year.
13:15	End of Workshop