DAVID SCHUM, GHEORGHE TECUCI, MIHAI BOICU

Analyzing Evidence and its Chain of Custody: A Mixed-Initiative Computational Approach

INTRODUCTION

Intelligence analysts encounter a wide variety of items of evidence provided by an array of different sources. Some of these sources are human assets or informants; other sources are sensing devices of various kinds. Of great concern is the extent to which the events revealed in these evidence items can be believed. There is always the possibility that information we receive has been deliberately contrived to mislead us. A human informant may have any number of reasons for fabricating evidence in order to deceive us. It is also possible that our human sources or sensing devices are simply erroneous in their observations. Whether by deliberate fabrications or observational mistakes there is always the possibility of our being misled in the conclusions we draw from intelligence evidence.

Dr. David Schum *holds the rank of Professor in the Systems Engineering and Operations Research Department in the Volgenau School of Information Technology and Engineering, and in the School of Law, at George Mason University. He is also Honorary Professor of Evidence Science, University College London.*

Dr. Gheorghe Tecuci *is Professor of Computer Science in the Volgenau School of Information Technology and Engineering and Director of the Learning Agents Center at George Mason University, and Visiting Professor and former Chair of Artificial Intelligence at the US Army War College.*

Dr. Mihai Boicu *is Assistant Professor of Applied Information Technology and Associate Director of the Learning Agents Center in the Volgenau School of Information Technology and Engineering, George Mason University.*

Unfortunately, there is another way we can easily be misled and it concerns what we ourselves do with the evidence between the time the original evidence is acquired from a source and when intelligence analysts receive final reports of the substance of this evidence. In a few cases intelligence analysts may interact directly with assets or informants or they may receive original sensor records or various other kinds of tangible objects. In many cases, however, the original evidence from some source is processed in a variety of ways either by persons having skills necessary at some processing step or by devices that perform these processing steps automatically. Here we have borrowed an important concept from the field of law to describe these intermediate processing steps; this concept is that of a chain of custody. As we will describe in detail, a chain of custody refers to the persons or devices having access to the original source evidence, the time at which they had such access, and what they do to the original evidence when they had access to it. The important point here is to consider what was done to the original evidence and the extent to which what the analyst finally receives is an authentic and complete account of what an original source provided. Uncertainties arising in chains of custody of intelligence evidence are not always taken account of. One result is that we can often mislead ourselves about what evidence is telling us. The original evidence may be altered in various ways at various links in chains of custody. This can mean that the evidence received by the analyst is not the same as the original evidence provided by its source.

One major trouble is that the chain of custody of some item of intelligence evidence depends on what form the original evidence takes. As we will discuss, evidence can be testimonial assertions from a human source based on observations this source allegedly made. But it can also be one of a wide variety of tangible evidence items either in the form of records of our own sensor observations or of other objects provided for us by various external sources. The point here is that possible uncertainties are introduced at each link in a chain of custody through which some item of intelligence evidence passes. Identifying and assessing these sources of uncertainty, if they are indeed taken into account, is a very complex activity. Add to this the uncertainties associated with the credibility of the original sources themselves, and so analysts have an extremely difficult time assessing the extent to which they can believe the events reported in the evidence they receive.

However, there is a computer-based cognitive assistant that can help analysts perform the difficult task of assessing the extent to which the event(s) reported in some item of intelligence evidence can be believed. We have developed a system called Disciple-LTA, where LTA means "Learner, Tutor and Assistant". As we will describe, this system allows analysts to perform credibility assessments for original sources as well as assessing possible uncertainties arising at links in the chains of custody through which intelligence evidence passes. A major objective of this paper is to present examples of the use of Disciple-LTA in assessing the believability of intelligence analysis. One major feature of this system is that it allows an analyst to decompose, or to "drill down", these assessments to various more detailed levels of analysis depending upon the time the analyst has to make detailed judgments and on the availability of information necessary to make these judgments. We begin by a brief account of forms of evidence and their credibility attributes and an account of what might be encountered in chains of custody.

FORMS OF EVIDENCE AND THEIR BELIEVABILITY ATTRIBUTES

As far as the substance or content of evidence is concerned, there is a near infinite variety of it. However, there is a way of categorizing evidence into a small class of distinguishable forms of evidence that recur and do not depend on the substance of the evidence. This "substance-blind" categorization of evidence is described in other works [Schum, 2001, 114 - 130; Anderson, Schum, Twining, 2005, 71 - 77]. For our present purposes we need only mention two of these forms of evidence: testimonial and tangible.

Testimonial Evidence. So much of intelligence analysis depends upon what human sources, assets, or informants tell us that have observed in situations of interest. Some of these sources may be foreign nationals we have recruited; but others may be members of our own military or governmental organizations. In any case, such reports are commonly called HUMINT and consist of testimony from these sources. It is true, of course, that our human assets also provide us with other things that we will consider when we discuss tangible evidence. As far as the sources of HUMINT are concerned we have two quite distinct matters of interest. The first concerns the competence of these human sources. Assessments of the competence of a source require answers to two important questions. First, did this source have access to, or did actually observe, the events being reported? If it is believed that a source did not have access to, or did not

actually observe the events being reported, we have very strong grounds for suspecting that this source fabricated this report or was instructed what to tell us. Second, we must have assurance that the source understood the events being observed well enough to provide us with an intelligible account of these events. So, access and understanding are the two major attributes of a human source's competence. Assessments of human source credibility require consideration of entirely different attributes.

The credibility of a source of HUMINT testimony involves consideration of three attributes: veracity [or truthfulness], objectivity, and observational sensitivity under the conditions of observation. Here is an account of why these are the major attributes of testimonial credibility. First, is this source telling us about an event he/she believes to have occurred? This source would be untruthful if he/she did not believe the reported event(s) actually occurred. So, this question involves the source's veracity. The second question involves the source's objectivity. The question is: did this source base a belief on sensory evidence received during an observation, or did this source believe the reported events occurred either because this source expected or wished them to occur? An objective observer is one who bases a belief on the basis of sensory evidence instead of desires or expectations. Finally, if the source did base a belief on sensory evidence, how good was this evidence? This involves information about the source's relevant sensory capabilities and the conditions under which a relevant observation was made.

Answers to these competence and credibility questions require information about our human sources. But one thing is abundantly clear: the competence and credibility of HUMINT sources are entirely distinct. Competence does not entail credibility, nor does credibility entail competence. Confusing these two characteristics invites inferential disaster. We have encountered several works on intelligence analyses in which the following assertion was made: "We can believe what this source has told us because he had good access". This is a glaring non sequitur; the source may have had all the access in the world but be lying through his teeth about what he observed.

Tangible Evidence. There is an enormous variety of tangible evidence that we may define as evidence which can be directly examined by someone to see what events it reveals. Objects, documents, images and other sensor records, charts, tables, maps, and diagrams are all examples of tangible evidence items. But there is a useful way in which we can further categorize tangible evidence. It is often important to distinguish between real tangible evidence and demonstrative tangible evidence. This distinction is often

made in the field of law [e.g. Lempert, Gross, & Liebman, 2000, 1146 - 1148]; it can also be very helpful in intelligence analysis. Real tangible evidence refers to the objects or things themselves that may be relevant in an intelligence analysis. Examples include weapons or weapon components, such as fragments of an IED; original documents, other objects such as uniforms, body parts, toxic chemical samples or soil samples of various kinds such as those obtained in MASINT. In some instances video or auditory recordings of events at the time they occurred are taken as real evidence. Demonstrative tangible evidence does not concern things themselves but only representations or illustrations of these things. Examples include diagrams, maps, scale models, statistical or other tabled measurements, and sensor images or records of various sorts such as IMINT, SIGINT, and COMINT. For example, a photo of a person is not the same as the person himself but only a representation of this person. A hand-drawn map is only a representation of some locality.

Real tangible evidence has only one major credibility attribute: authenticity. Is this object what it is represented as being or is claimed to be? There are as many ways of generating deceptive and inauthentic evidence as there are persons wishing to generate it. Documents, or written communications may be faked, captured weapons may have been altered, and photographs may have been altered in various ways. One problem is that it usually requires considerable expertise to detect inauthentic evidence. Further, different kinds of real tangible evidence require different areas of expertise. For example, it may require quite different expertise to detect a forged document than it does to detect an altered photo or a deceptive weapon component. Concern about such matters is an obvious processing step in the chain of custody of real tangible evidence.

Demonstrative tangible evidence has three credibility attributes. The first concerns its authenticity. So, both real and demonstrative tangible evidence have this crucial credibility attribute. For example, suppose we obtain a hand drawn map from a captured insurgent showing the locations of various groups in his insurgency organization. Has this map been deliberately contrived to mislead our military forces or is it a genuine representation of the location of these insurgency groups? The second major attribute is especially relevant to various forms of sensors that provide us with many forms of demonstrative tangible evidence. We are naturally concerned about the reliability of these sensors and whether they would yield the same information if they were exercised again under the same conditions. The reliability of a sensing device

certainly concerns its quality in addition to how well it has been maintained. The third credibility attribute concerns the accuracy of the representation provided by the demonstrative tangible item. We would be as concerned about the accuracy of the hand-drawn map allegedly showing insurgent groups locations as we would about the accuracy of a sensor in detecting traces of some physical occurrence. Assessments of these attributes for real and demonstrative tangible evidence requires a variety of information that an analyst will probably not always have. Such information may or may not be available to persons who, at various links in chains of custody of tangible evidence, may also be concerned about these credibility attributes.

CHAINS OF CUSTODY FOR INTELLIGENCE EVIDENCE

Intelligence analysts have various questions about evidence they receive that are as important as they are obvious. One vital question concerns the authenticity of this evidence, whether it is tangible or testimonial in nature. As noted, we can be misled by our source of evidence. But, some very important authenticity issues arise after we receive evidence from some source and it is in our possession. If the item of evidence is testimonial HUMINT, the analyst asks: Is the account I have received of this testimony an accurate and complete account of what the asset or informant actually said? If the item of evidence is tangible in nature, such as an object or image of something from a sensing device, the analyst asks: Is this object, or some image or account of it, identical to the one that was actually received from one of our sources, or is it a faithful representation of the original item? A crucial step in answering such questions involves having knowledge about the chain of custody through which the testimonial or tangible item has passed en route to the analyst who is charged with assessing its relevance, credibility, and inferential force or weight.

Basically, establishing a chain of custody involves identifying the persons and devices involved in the acquisition, processing, examination, interpretation, and transfer of evidence between the time the evidence is acquired and the time it is provided to intelligence analysts. Lots of things may have been done to evidence in a chain of custody that may have altered the original item of evidence, or have provided an inaccurate or incomplete account of it. In some cases, original evidence may have been tampered with in various ways. Unless these difficulties are recognized and possibly overcome, intelligence analysts are at risk of drawing quite erroneous conclusions from

the evidence they receive. They are being misled, not by our original sources of evidence, but by the activities of our own persons or devices who do various things to incoming intelligence evidence.

In civilian and military courts, proponents of evidence, for either side of the matter in dispute, are required to verify the chain of custody of tangible evidence before it is admitted at trial. In many cases, evidence gathered is passed from one person to another, each of whom may examine and process the evidence in various ways. In many situations, proponents are required to select experienced and credible persons who serve as evidence custodians. The major task for these persons is to establish the chain of custody of evidence keeping records of who gathered the evidence, the persons who had access to the evidence, the times at which they had access, and what these persons did with the evidence while they had access to it. A very good account of questions regarding the chains of custody of evidence in our courts is to be found in the book by Lempert, Gross, & Liebman [2000, 1167 - 1172].

Now, we are of course not privy to the actual chains of custody of various forms of intelligence evidence in any of our intelligence organizations. And we do not know whether there are any appointed evidence custodians in these organizations as there are in our legal system. However, we can offer accounts of chains of custody of evidence that seem reasonable and necessary for different forms of evidence. In our examples of how Disciple-LTA can assist analysts to establish the believability of evidence, we have established conjectural accounts of chains of custody for an item of testimonial and an item of tangible evidence in order to illustrate the virtues of Disciple-LTA and how it can assist the intelligence analyst to make these very difficult believability assessments.

First, suppose we have an analyst who is provided with an item of testimonial evidence by an informant who speaks only in a foreign language. We assume that this informant's original testimony is first recorded by one of our intelligence professionals; it is then translated into English by a paid translator. This translation is then edited by another intelligence professional; and then the edited version of this translation is transmitted to an intelligence analyst. So, there are four links in this conjectural chain of custody of this original testimonial item: recording, translation, editing, and transmission. Various things can happen at each one of these links that can prevent the analyst from having an authentic account of what our source originally provided.

Then, suppose that an analyst is provided with an account of a tangible item in the form of a digital photo. This photo has been taken by one of our foreign assets. We note that the analyst may see a copy of the photo itself or just a written account of the events recorded in this photo. Suppose in this case the analyst only receives a written account of what this original photo revealed. We have supposed that this digital photo is first transferred to the computer of one of our intelligence professionals; it is then transmitted to a photo interpreter; the image is interpreted by this person; and then the written interpretation of this photo is then transmitted to the analyst. So, in this conjectural chain of custody there is a transference link, an interpretation link, and two transmission links. At any of these links there are possible reasons why what the analyst receives is not an authentic account of what the asset's original photo depicted.

With these evidential and chain of custody ideas in mind, we can now show how Disciple-LTA can assist intelligence analysts to assess the many sources of uncertainty associated with the authenticity of evidence they receive. We first provide a case study illustrating the matters we have just mentioned.

A CASE STUDY

The cover story for this hypothetical case involves an experienced analyst named Clyde who is involved with intelligence analyses concerning matters in Iraq. Clyde's present inferential problem involves an Iraqi named Emir Z., a respected official of the existing government in Iraq. Emir Z. has publicly argued on many occasions about the necessity for stopping the sectarian violence that has plagued Iraq and coalition efforts to achieve stability in this country since the US and coalition intervention in 2003. Clyde's present problem is that he wonders how respectable Emir Z. really is. Clyde has evidence that Emir Z. has been in contact in Iran with representatives of the Iranian Islamic Revolutionary Guards Corp [IRGC]. We **already** have a variety of strong evidence that the IRGC has been involved in supplying weapons, training, and intelligence to various Shiite militia groups in Iraq. This has certainly not contributed to stability in Iraq and is against the interests of the coalition forces in Iraq. So, Clyde entertains the hypothesis H_1: that Emir Z, is collaborating with the IRGC [i.e. he is not the respected official we have believed him to be].

So far Clyde has two items of evidence bearing on H_1:

1. He first has an item of testimonial evidence from a source code-named Wallflower who reports that five days ago he saw Emir Z. leaving a building in Ahwaz, Iran in which the IRGC has offices. Wallflower, an Iranian national, issued his report in the Farsi language that was recorded and then translated into English by a paid interpreter. Then an edited version of this translation is recorded and transmitted to Clyde.
2. Then Clyde receives an item of tangible evidence in the form of a photograph taken of Emir Z. eight days ago at an IRGC Qods Force base outside Dezful in Iran. This photo was taken by another source code-named Stovepipe. The identification of Emir Z. in this photo was verified by one of the US intelligence professionals who has had contact with Emir Z. We will assume that Clyde receives this photo together with a written account of what this photo revealed. But we also allow for the possibility that Clyde receives only a written account of the contents of this photo.

Here is a summary account of the inferential problems Clyde faces as he attempts to assess how believable he **imagines** these two items of evidence to be. It is common to talk about the credibility of evidence (Schum, 2001). However, we think that it is more appropriate to talk about the believability of evidence, since it will include both credibility and competency considerations. We begin by examining the credibility and competence of Clyde's original sources: Wallflower and Stovepipe.

Wallflower provides testimonial evidence in the form of an assertion he made concerning Emir Z. leaving the IRGC building in Ahwaz, Iran. Wallflower says he based this assertion on his direct observation of these events five days ago. In deciding whether to believe Wallflower, Clyde must first consider both Wallflower's competence and his credibility (Schum, 2001; 2007). Wallfower's competence involves his access and his understanding. The basic access question involves asking whether Wallflower was actually in a position to observe what he tells us. The understanding question asks whether Wallflower knew enough about what he was observing to give us an intelligible account of what he observed. His credibility involves the veracity, objectivity, and observational sensitivity attributes we mentioned above

Stovepipe, on the other hand, supplies tangible evidence in the form of a photo he says he took eight days ago of Emir Z. at an IRGC base outside Dezful, Iran. Considering

Stovepipe himself, Clyde must first consider Stovepipe's competence. What evidence does Clyde have that Stovepipe was actually in Dezful at the time he says he took the photo? In addition, what evidence does Clyde have that Stovepipe knew the person he was photographing? Clyde also has one credibility attribute for Stovepipe to consider, namely his veracity. Was Stovepipe truthful in telling us when, where, how, and why he took this photo. We will assume that we are treating the photo provided by Stovepipe as being demonstrative tangible evidence. There are several reasons why this makes sense. First, we have the believability of the photo itself to consider. Is this photo authentic: is it what it is represented as being, namely Emir Z at the IRGC base outside Dezful, Iran? Second, has this evidence come from a reliable sensing device that would supply us with repeatable information? Third, is the evidence accurate in allowing Clyde or anyone else to tell whether it was really Emir Z. in the photo? These three maters all concern the credibility of the photo itself.

But Clyde has other sources of uncertainty to worry about, ones that concern the chains of custody through which these two intelligence items have passed before Clyde receives account of these items. Here we present two conjectural chains of custody, one for the testimonial item from Wallflower and one for the tangible item from Stovepipe. The reader may quickly note other links in these chains of custody that we have overlooked, or have different labels for the ones we have included. Not being privy to any actual chains of custody of intelligence evidence, our conjectural chains of custody may lack realism. But our claim is that they are plausible enough to illustrate the kinds of uncertainties encountered in chains of custody of intelligence evidence and also to illustrate how Disciple-LTA can assist analysts in making these kinds of assessments.

First, Clyde has not heard Wallflower's original testimony and could possibly not have understood it unless Clyde speaks Farsi. We have identified a case officer named Bob who may only speak limited Farsi. Bob records what Wallfower has testified on a Sony recording device. This recording is transmitted to a paid foreign national named Husam A. who speaks fluent Farsi. Husam's written translation of Wallfower's testimony about Emir Z. is then transmitted to a reports officer named Marsha. Marsha edits Husam's translated version of Wallflower's testimony and prepares her written edited version for transmission over a [fictitious] system we will call SN247. What Clyde receives is Marsha's edited version of Husam A.'s translation of Wallflower's original testimony. This is a tangible item that is only an account of what Wallfower originally

said. This account can only be regarded as demonstrative tangible evidence whose authenticity, reliability, and accuracy are at issue due to the uncertainties arising at each link in the chain of custody through which Wallflower's orginal testimonly has passed.

Now consider the tangible photo that Stovepipe has provided. First, suppose Stovepipe used an Olympus # ABC digital camera to take the photo of Emir Z. We suppose that Stovepipe had some means for transferring this digital photo to case officer Bob's laptop computer. Bob then transmits this stored digital photo to a photo interpreter we shall name Mike. Mike examines the photo to assess its authenticity, and he also verifies that the person depicted in the photo is Emir Z. Mike prepares a written account of his analysis of this photo. Mike then transmits his written account of this photo, and possibly a copy of the photo itself over our [fictitious] system SN 247. This written account of the photo, and possibly a copy of the photo, is eventually routed to Clyde for his analysis of it.

The point of this case study is to illustrate the array of uncertainties our analyst Clyde encounters in his efforts to assess the extent to which he and others might believe the testimonial and tangible evidence he has received from Wallflower and Stovepipe. Some of these uncertainties concern these two sources themselves, and others concern what was done to their original evidence in their chains of custody. We now consider how Disciple-LTA can assist Clyde in coping with these many uncertainties.

1) A Chain of Custody for Testimonial Evidence

As we just noted, several things were done to Wallflower's and Stovepipe's evidence before it could be considered by Clyde. Different people had custody of these two items of evidence and did different things to them before Clyde actually saw them. Figure 1 show a specific (hypothetical) example of what might be involved in the chain of custody of Wallflower's original testimonial evidence. The major issue here is the extent to which Clyde can believe what he is told Wallflower said. This belief rests not only on evidence regarding Wallflower's competence and credibility, but also on the competence and credibility issues raised by what was done to Wallflower's original report about Emir Z. before Clyde received a report of what Wallflower testified. First and foremost, we have the competence and credibility of our primary source of this testimony, Wallflower. Then we are concerned with how authentic is the account of

Wallflower's testimony that is provided for the person, Clyde, who will use this account? Are we sure that this account actually records, completely and accurately, what Wallflower reported? Bear in mind here that Clyde has never seen or talked to Wallflower himself. Here is a representation of a possible chain of custody for testimonial evidence such as Wallflower's.

In the example from Figure 1 we have three identified persons involved in the chain of custody of Wallflower's report: a case officer Bob, a translator Husam A., and a reports officer Marsha. Now one thing about this fictitious example is that the analyst, Clyde, may or may not know the identities of these three persons. And, in actual situations, there may be more or different persons involved in chains of custody. The top part of Figure 1 shows the successive transformations suffered by Wallflower's original testimony (called EVD-Wallflower-1) until it reaches Clyde, who actually receives the piece of evidence called EVD-Wallflower-5. The bottom part of Figure 1 shows the competence and credibility issues that can arise regarding the persons and the devices involved in this example.

Here comes the interpretation of the chain of custody shown in Figure 1 and the believability-related issues regarding the processes at each link in this chain.

First Wallflower's testimony (EVD-Wallflower-1) was tape-recorded by the case-officer Bob who interacts with Wallflower. So, we have natural concerns about the fidelity and reliability of this tape-recording, as well as about Bob's competence and veracity. Among other things, is the recording understandable and complete? Was all of Wallflower's testimony on the recording and no gaps appear in it? Clyde would also be interested to know whether Wallfower provided his report voluntarily or whether he was asked to report on Emir Z. by Bob. This is quite important since if Wallflower gave this report voluntarily and we believe he is being untruthful, Clyde has to ask why Wallflower told Bob this particular lie in preference to any of the others he might have told. The same question will arise for Stovepipe's evidence.

As we have specified, Wallflower speaks only Farsi and not English, and Husam A. has translated his recorded testimony (i.e. EVD-Wallflower-2) into English. We have concerns here about the competence and credibility of Husam A. Competence involves not only knowledge of Farsi and English, but also knowledge of the subject matter being translated. The translated account of Wallflowers original testimony (i.e. EVD-Wallflower-3) is then edited by Marsha.

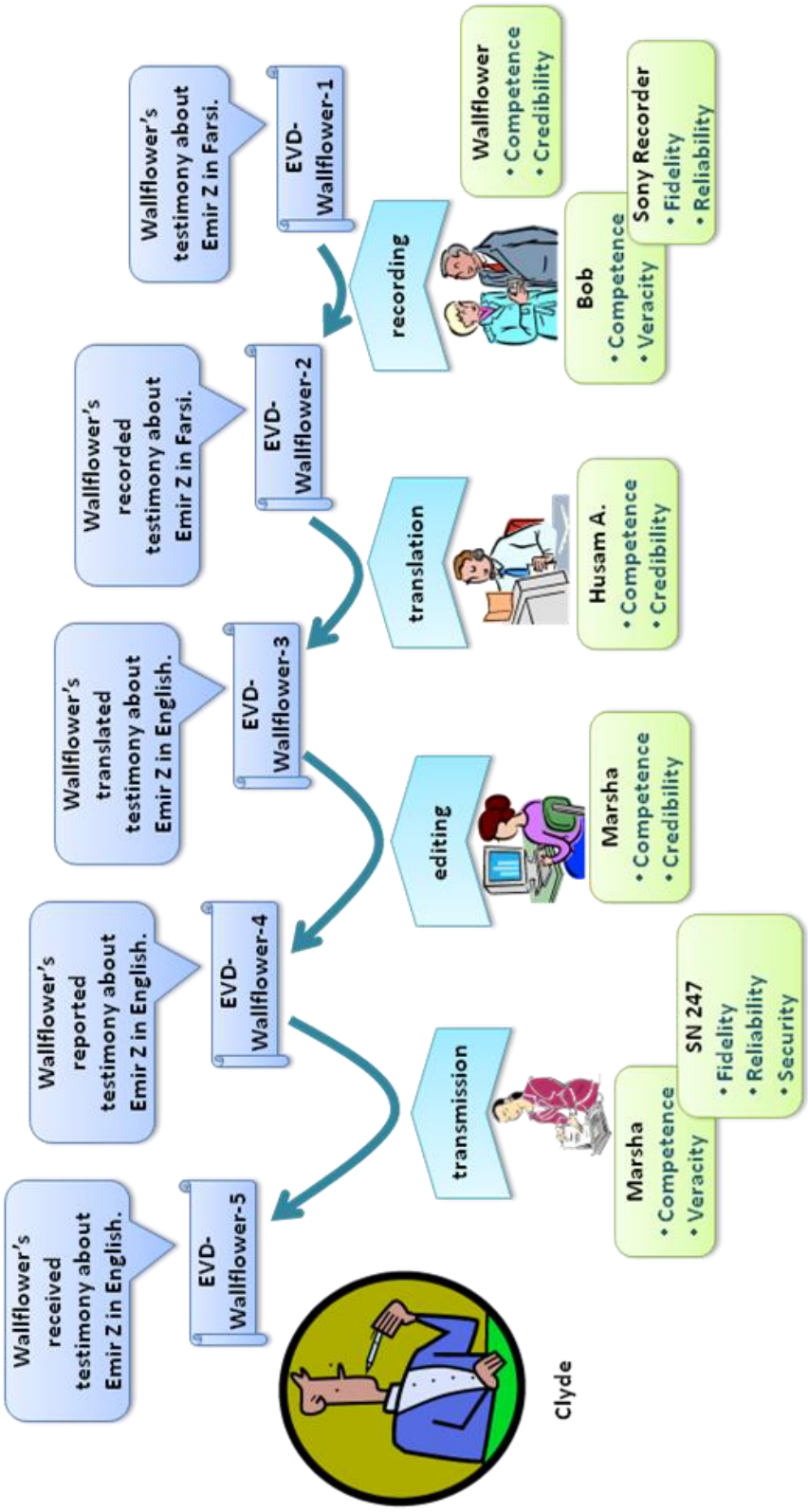

Figure 1: Chain of custody of Wallflower's testimony and the processes in this chain.

We may have here concerns about Marsha's competence and credibility.

Finally, this recorded, translated and edited account of Wallflower's testimony (i.e. EVD-Wallflower-4) is transmitted through a computer network to Clyde and possibly to many others interested persons. We have here concerns both about the competence and credibility of the person who performed the transmission, and also about the fidelity, reliability, and security of the transmission.

2) Chain of Custody for Demonstrative Tangible Evidence

Unfortunately, regarding the photo of Emir Z., allegedly taken in Dezful, Iran eight days ago, we have two possibilities to consider. We have to consider whether Clyde was given a copy of this photo to examine himself, or whether he was just given a written account of what this photo depicted. The major trouble, of course, is that the chains of custody will be different in these two cases. So, we will make some conjectures about what the chains of custody might look like in both of these cases. The first is where Clyde is given the photo himself to examine; the second is where he is just given a written account of what is in Stovepipe's photo.

Case A) Chain of Custody for the Photo Given Directly to the Analyst

We will begin with the case in which Clyde sees Stovepipe's photo itself or, more than likely, a copy of Stovepipe's original photo. The corresponding chain of custody involves the persons and processes shown in Figure 2. The top part of Figure 2 shows the successive transformations suffered by Stovepipe's original photo of Emir Z. (called EVD-Stovepipe-1) until it reaches Clyde (as EVD-Stovepipe-5). The photo was transferred by Bob on his laptop, and then transmitted electronically to Mike's computer. Mike interpreted the photo and then transmitted both the photo and its interpretation to Clyde. The bottom part of Figure 2 shows the competence and credibility issues that can arise regarding the persons and the devices involved in this example.

We are going to suppose that Stovepipe took the picture using a digital camera. This will eliminate the necessity of considering who and where the photo was developed. We will also assume that Stovepipe, who knows Emir Z., was instructed to follow Emir Z. eight days ago in Dezful, to see where he went that day.

We have also assumed that Stovepipe was able to visit Bob bringing his digital camera with him. There are, of course, other means by which Stovepipe might have communicated with Bob. If Stovepipe had a laptop computer he could have e-mailed the message to Bob, who could have been anywhere in Iran or Iraq. But this would add additional risks involving the e-mail being intercepted by the Iranian IRGC. Sure, there are risks associated with Stovepipe's meeting personally with Bob. It took Stovepipe eight days between the time he took the photo and the time he delivered it to Bob. How Stovepipe actually got the photo to Bob is interesting and will eventually bear on Stovepipe's competence and the authenticity of the photo. Maybe the procedures necessary for Stovepipe to communicate directly with Bob are very complex and have been designed to reduce the risks associated with this direct communication. For example, suppose Bob is in Baghdad, Iraq but meets with Stovepipe in Al Amara, Iraq. Both cities are near the Iraq-Iran border about 80 miles from each other. Perhaps it takes several days for Stovepipe to communicate with Bob and then arrange the cover necessary to go into Iraq. These are all matters that bear upon Stovepipe's competence and may also concern the authenticity of the photo.

But the major assumption underlying this scenario concerns whether or not we can say that Clyde is provided with the original photo that Stovepipe alleged took. This involves the assumption that the image Bob uploaded on his computer and then transmitted it to Mike was not altered in any way, nor was the same image that Mike transmitted to Clyde. If the image that Clyde received had exactly the same pixels as the one on Bob's computer, we could probably say that Clyde received the same original photo that Bob received from Stovepipe.

Case B). The Analyst Receives Only a Written Description of the Photo

This second case is interesting for the following reason. We are treating the photo as being demonstrative tangible evidence since it is just a possible representation of Emir Z. being at Dezful eight days ago. Then, if Clyde is only given a written account of this photo, this is only demonstrative evidence of Stovepipe's original demonstrative evidence. So, in cases such as this, we have a chain of demonstrative evidence involving two or more sources.

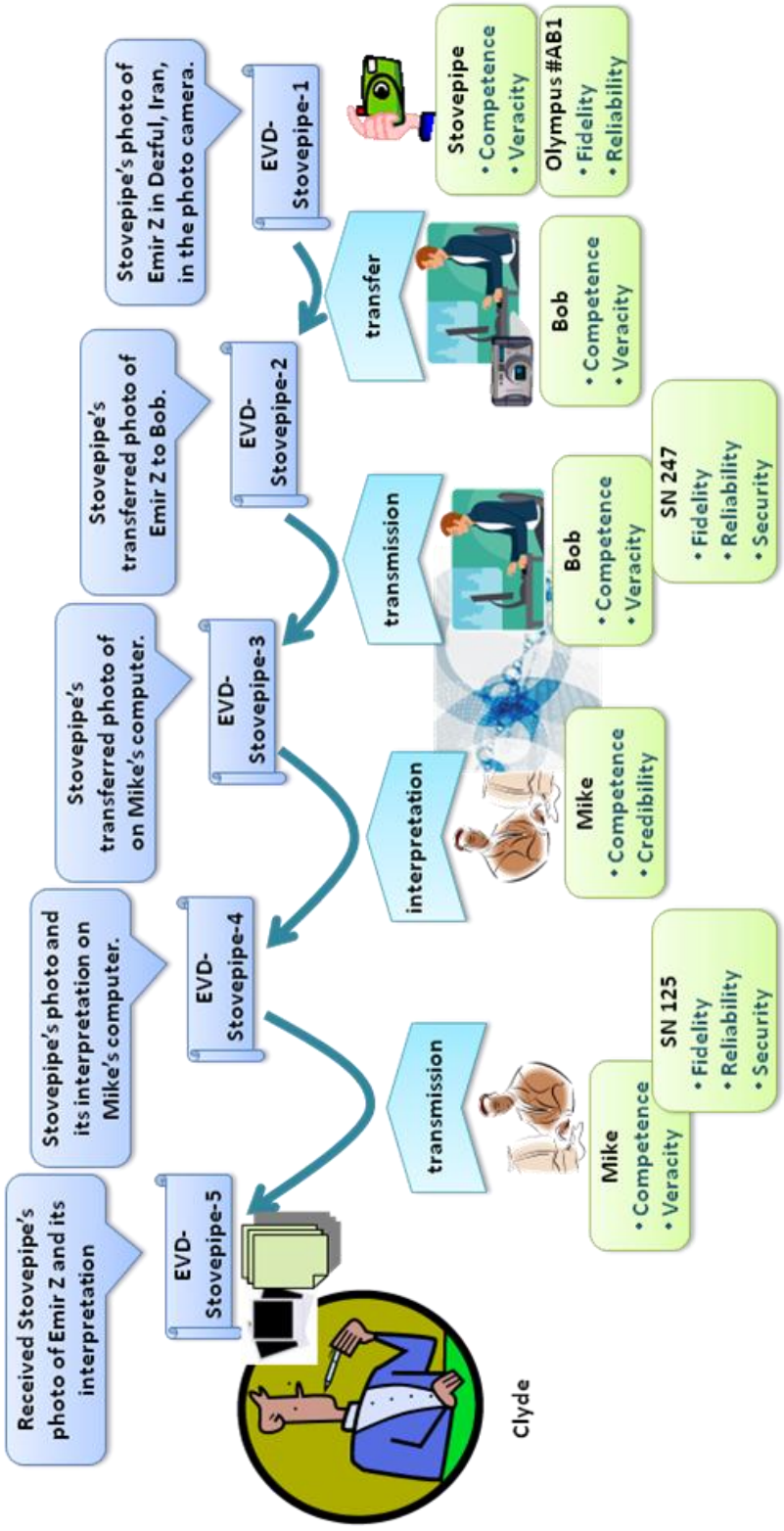

Figure 2: Chain of custody of demonstrative evidence sent to Clyde.

The above discussion shows how complex are the processes of analyzing the likelihood of hypothesis H_1: that Emir Z, is collaborating with the IRGC, even when we have just a small amount of evidence. However, for a good analysis, one would have to consider many more pieces of evidence, and to consider both favoring and disfavoring evidence. Unfortunately, the complexity of the analytic process grows so much with the addition of new pieces of evidence that all the involved probabilities cannot be assessed. There is simply not enough time for the analyst to assess them or evidence necessary to support these assessments is not available.

However, we now describe how our cognitive assistant Disciple-LTA (Tecuci et al., 2005; 2007a, 2007b) allows the analyst Clyde to generate the complex analysis involved in chains of custody of evidence. Clyde will be allowed to drill-down as much as he wishes; the can make assumptions concerning various verbal assessments of uncertainty, and to revise these assumptions in light of new evidence.

ASSISTING THE ANALYST: DISCIPLE-LTA COGNITIVE ASSISTANT

Disciple-LTA is a unique and complex analytic tool that integrates powerful capabilities for analytic assistance, learning and tutoring. At the basis of Disciple-LTA is an approach to software agent development where a subject matter expert, such as an intelligence analyst, can teach a Disciple software agent how to solve problems in a way that resembles how the expert would teach a student or a new analyst when solving problems in collaboration (Tecuci, 1998). The expert analyst will formulate a specific problem, such as “Assess the competence of Wallflower as the source of EVD-Wallflower-1”, and will explain the agent how she or he performs this analysis. From this specific analysis Disciple-LTA will learn general analysis rules that will allow it to solve similar problems, such as “Assess the competence of Stovepipe as the source of EVD-Stovepipe-1”, As Disciple-LTA learns from the expert analyst, it becomes an increasingly useful collaborator, solving the problems formulated by the analyst similarly to how the analyst would solve them himself or herself, only much faster. This allows the human analyst to act as the orchestrator of the analytic process, guiding the high level exploration of the reasoning space, while Disciple-LTA implements this guidance, together forming a very powerful team.

Critical to the success of Disciple-LTA as an analytic tool is the use of a systematic approach to evidence analysis which is both natural for a human analyst and

appropriate for an automatic software agent. This approach has a grounding in the problem reduction methods developed in Artificial Intelligence (Nilsson, 1971; Tecuci 1988), and in the argument construction methods provided by the noted jurist John H. Wigmore (1937), the philosopher of science Stephen Toulmin (1963), and professor David Schum (1999; 2001).

This approach facilitates the teaching of a Disciple-LTA agent by an expert analyst. It also allows a trained Disciple-LTA agent to act as a natural extension of the analytical reasoning capabilities of a human analyst, as well as teach new analysts in a way that is similar to how it was taught.

The following section illustrates the use of Disciple-LTA to automatically generate the believability analysis discussed in the previous sections.

1) Automatic Believability Analysis

Let us consider again the process illustrated in Figure 1. As discussed above, the believability of EVD-Wallflower-5 (Wallflower's received testimony about Emir Z.) is a function of the believability of EVD-Wallflower-4 and that of the transmission process; the believability of EVD-Wallflower-4 is a function on the believability of EVD-Wallflower-3 and that of the editing process; the believability of EVD-Wallflower-3 is a function on the believability of EVD-Wallflower-2 and that of the translation process; and, finally, the believability of EVD-Wallflower-2 a function on the believability of EVD-Wallflower-1 (the original testimony) and that of the recording process. Thus, the believability of the evidence received by Clyde is a function of the believability of the Wallflower's original testimony and the believability of the recording, translation, editing and transmission processes.

An important aspect of Disciple-LTA is that it has already been taught a great deal about the credentials of evidence and about the ingredients of believability assessments for tangible as well as testimonial evidence so that it can perform the above analysis, as discussed in the following. Disciple-LTA will use the names introduced in Figure 1 to refer to the considered pieces of evidence, such as EVD-Wallflower-5, EVD-Wallflower-4, etc.

Clyde's problem is to assess the believability of Wallflower-5 (i.e. Wallflower's alleged testimony about Emir Z., as received through the chain shown in Figure 1). This problem, which is shown in the upper-right side of Figure 3 is represented as:

"Assess the extent to which EVD-Wallflower-5 is believable." [1]

Disciple-LTA reduces this problem to two simpler hypothesis analysis problems, guided by a question and its answer:

How was EVD-Wallflower-5 obtained?
As the transmission of EVD-Wallflower-4 by Marsha with SN 247.

Therefore I have to

Assess the extent to which EVD-Wallflower-4 is believable. [2]
Assess the extent to which one can believe the transmission of EVD-Wallflower-4 into EVD-Wallflower-5 by Marsha with SN 247. [3]

Let us assume that the solutions of problems [2] and [3] are those shown at the bottom of Figure 3.

The believability of EVD-Wallflower-4 is likely. [4]
The believability of the transmission of EVD-Wallflower-4 into EVD-Wallflower-5 by Marsha with SN 247 is almost certain. [5]

These solutions are combined into the following solution of problem [1] (by taking the minimum of likely and almost certain):

The believability of EVD-Wallflower-5 is likely. [6]

Disciple-LTA uses five symbolic probabilities (i.e. remote, unlikely, even chance, likely, almost certain) to express the solutions of the problems. They correspond to the US National Intelligence Council's standard estimative language. However, this could easily be changed to consider more or fewer symbolic probabilities and to associate specific probability intervals with each of them (Kent 1994; Weiss, 2008). Notice also that some words appear in blue. They correspond to entities (such as Al Qaeda or nuclear weapons) that are represented in the knowledge base of Disciple-LTA (Tecuci et al, 2007b).

Figure 1 shows only the top part of the problem reduction and solution synthesis tree problem [1]. The problems from the bottom of Figure 3 (i.e. [2] and [3]) are themselves reduced, in a similar way, to simpler and simpler problems, guided by questions and answers. This problem reduction process continues until the resulting problems are simple enough to find their solutions. Then these solutions are successively combined, from bottom-up, to synthesize the solutions of the upper-level problems, until the solution of the top level problem is obtained. Overall, the entire reasoning tree is very large.

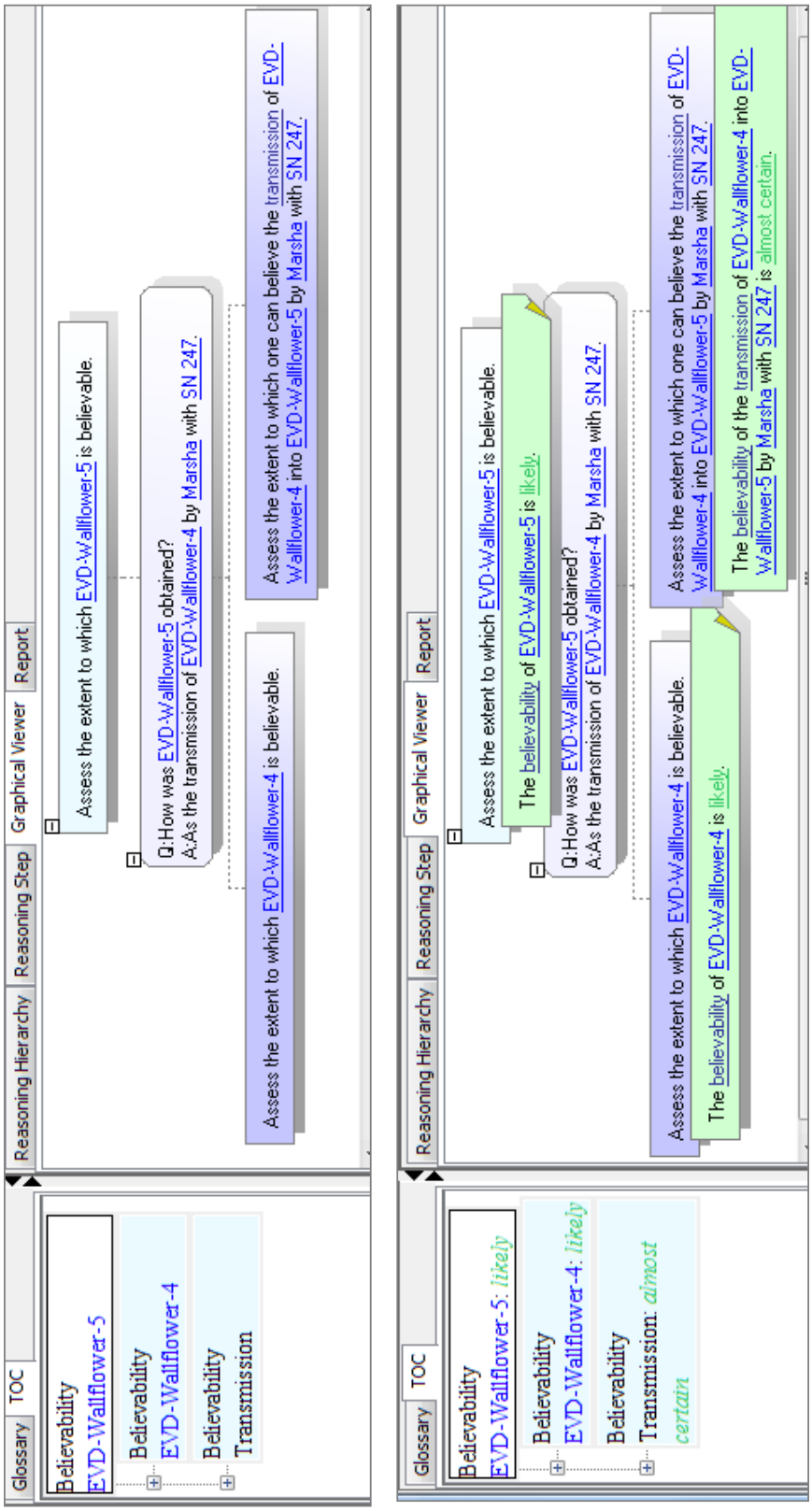

Figure 3: Hypothesis analysis through problem reduction and solution synthesis.

To help browse and understand such a complex analysis, Disciple-LTA displays a simplified version of it, as illustrated in the left-hand side of Figure 3. As one can see, under the short name of the initial problem and its solution (i.e. "Believability EVD-Wallflower-5: likely") Disciple-LTA lists the short names of the bottom problems from the right side of Figure 3 and their solutions:

Believability Wallflower-4: likely

Believability Transmission: almost certain

The left hand side of Figure 4 shows a summary of the believability analysis generated by Disciple-LTA for EVD-Wallflower-5, which corresponds to the scenario from Figure 1.

Because "Believability EVD-Wallflower-4" was selected in the left-hand side of Figure 4, the right hand side of this figure shows the detailed reduction of this problem.

The left hand side of Figure 5 shows the expansion of the analysis for "Believability EVD-Wallflower-1" which takes into account the competence and the veracity of Wallflower.

2) A Flexible Assumption-Based Analysis

As indicated above, the analyst may not have the time or the evidence to assess all the factors involved. In such a case Disciple-LTA allows him/her to make assumptions with respect to the solutions of the unsolved problems. As illustrated in Figure 6, the analyst may assume that the believability of all the processes involved in the chain of custody is almost certain, and concentrate his analysis on assessing the credibility of Wallflower. He may further make some assumptions about Walflower's competence, veracity, objectivity and observational sensitivity, and then Disciple-LTA will automatically estimate the overall believability of EVD-Wallflower-5. Yellow background in Figure 6 indicates that the enclosed solution is an assumption.

But the analyst can drill-down to analyze each of the processes from the chain of custody. For example, Figure 7 shows the analysis of the Recording performed by Bob. Disciple-LTA was able to automatically estimate the quality of the recording as "almost certain", based on its knowledge about the general fidelity and reliability of a Sony XYZ recorder. However, the believability of Bob was assumed by Clyde as "almost certain." Disciple-LTA also allows the analyst to investigate all sorts of what-if scenarios. For example, Figure 8 shows how Clyde may consider alternative values for the veracity of Husam A., the translator of Wallflower's testimony.

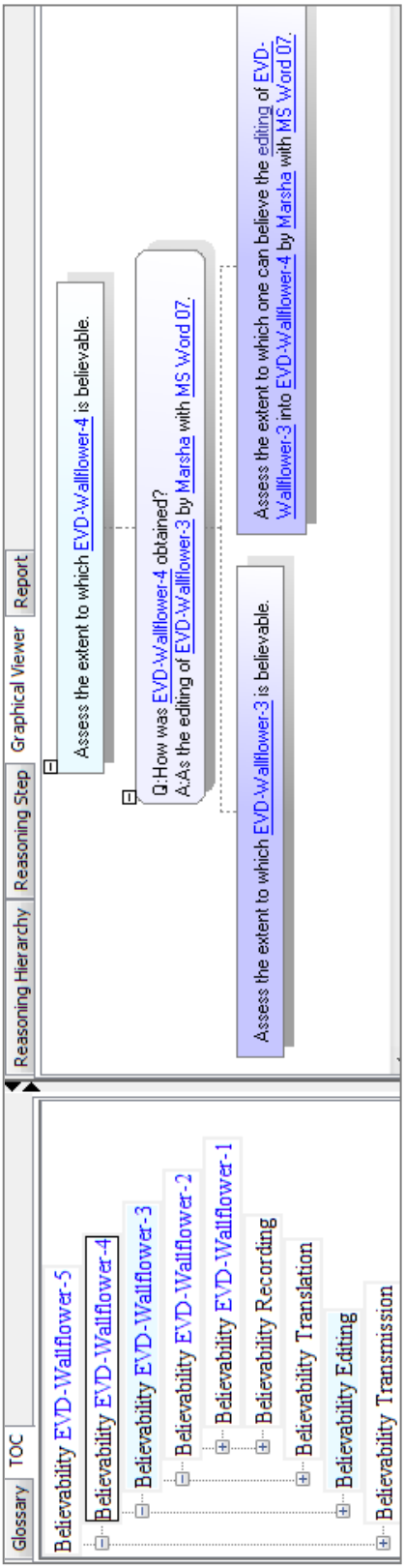

Figure 4: Overall believability analysis for the chain in Figure 1.

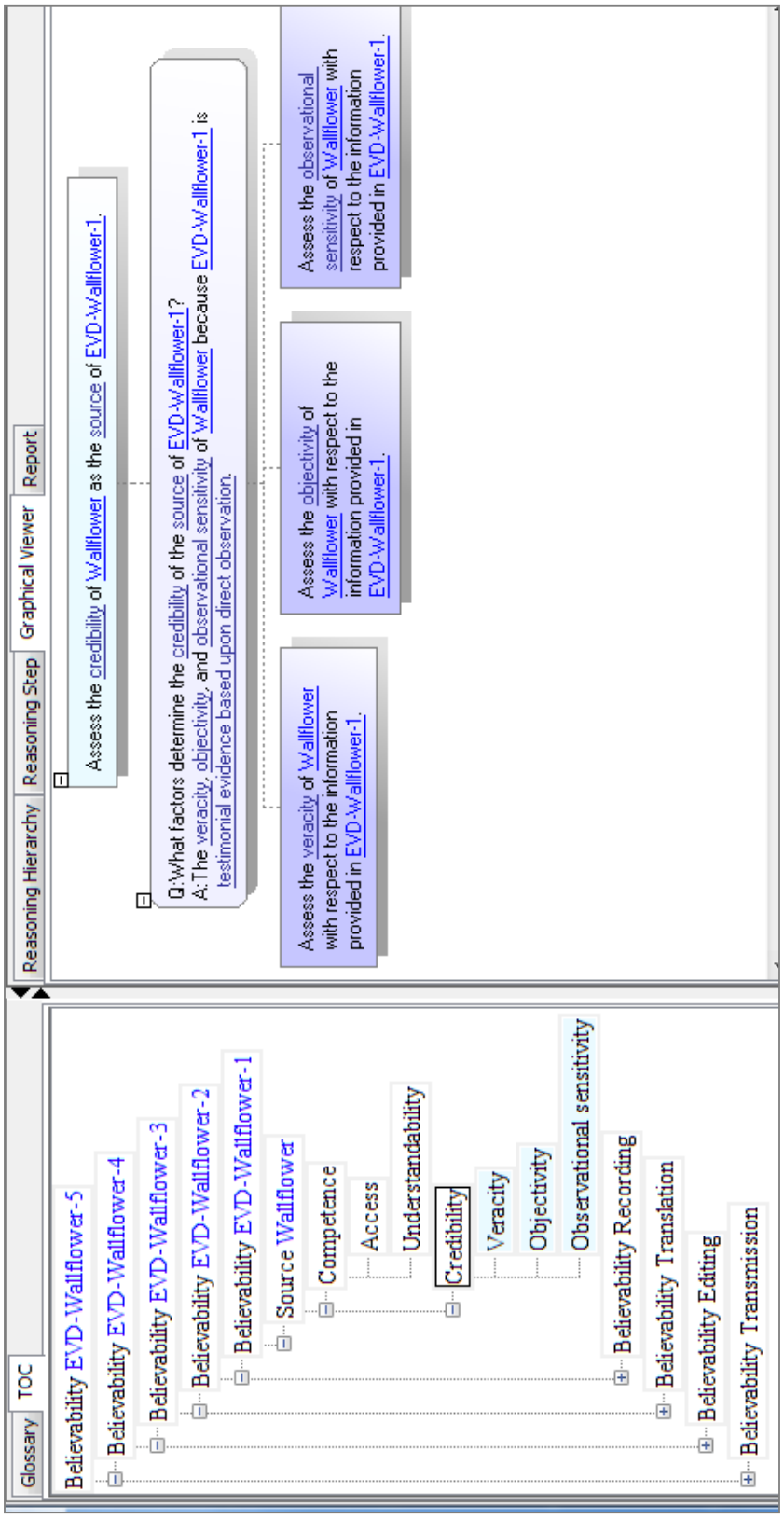

Figure 5: The details of the analysis of the believability of EVD-Wallflower-1.

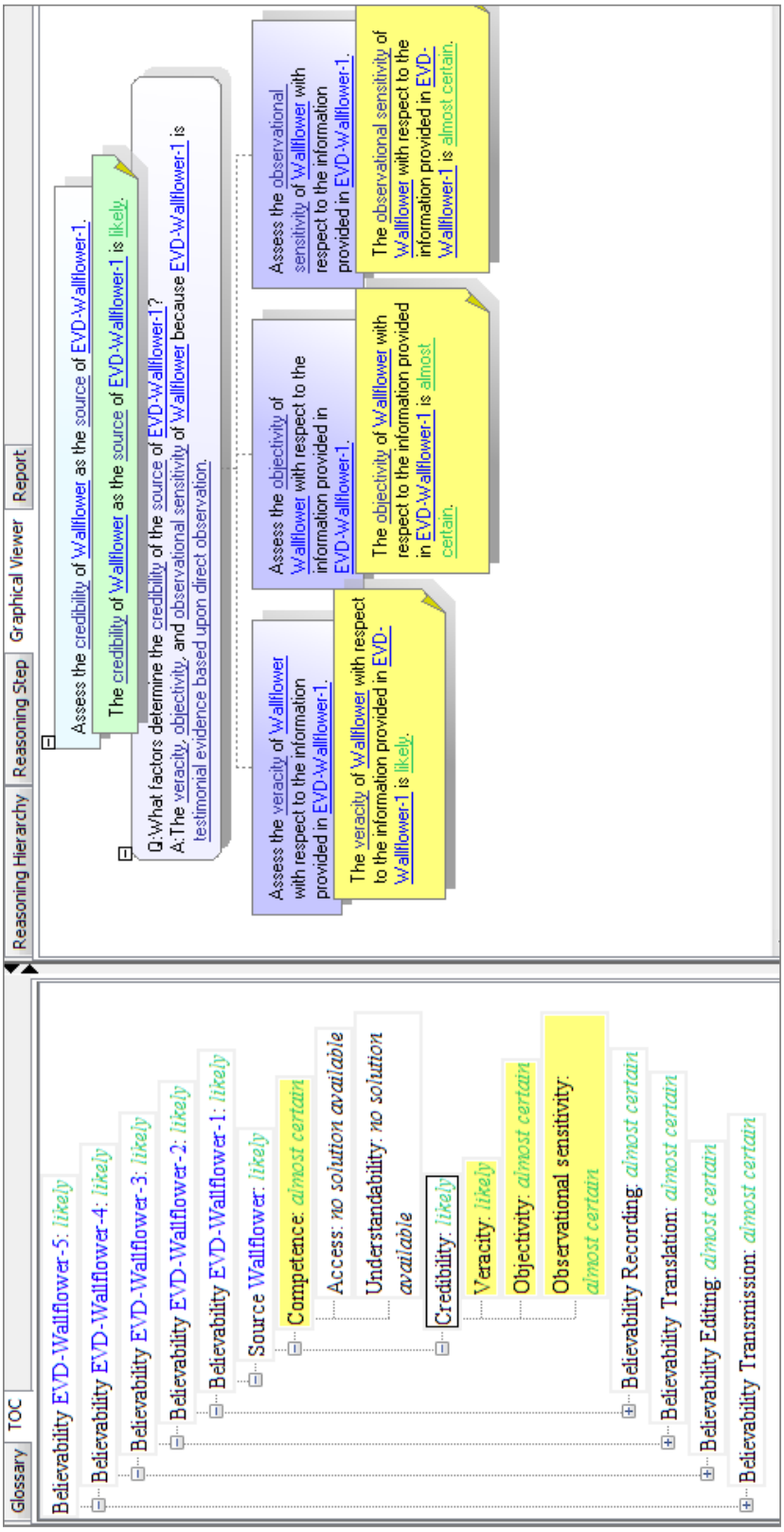

Figure 6: Assumption-based believability analysis.

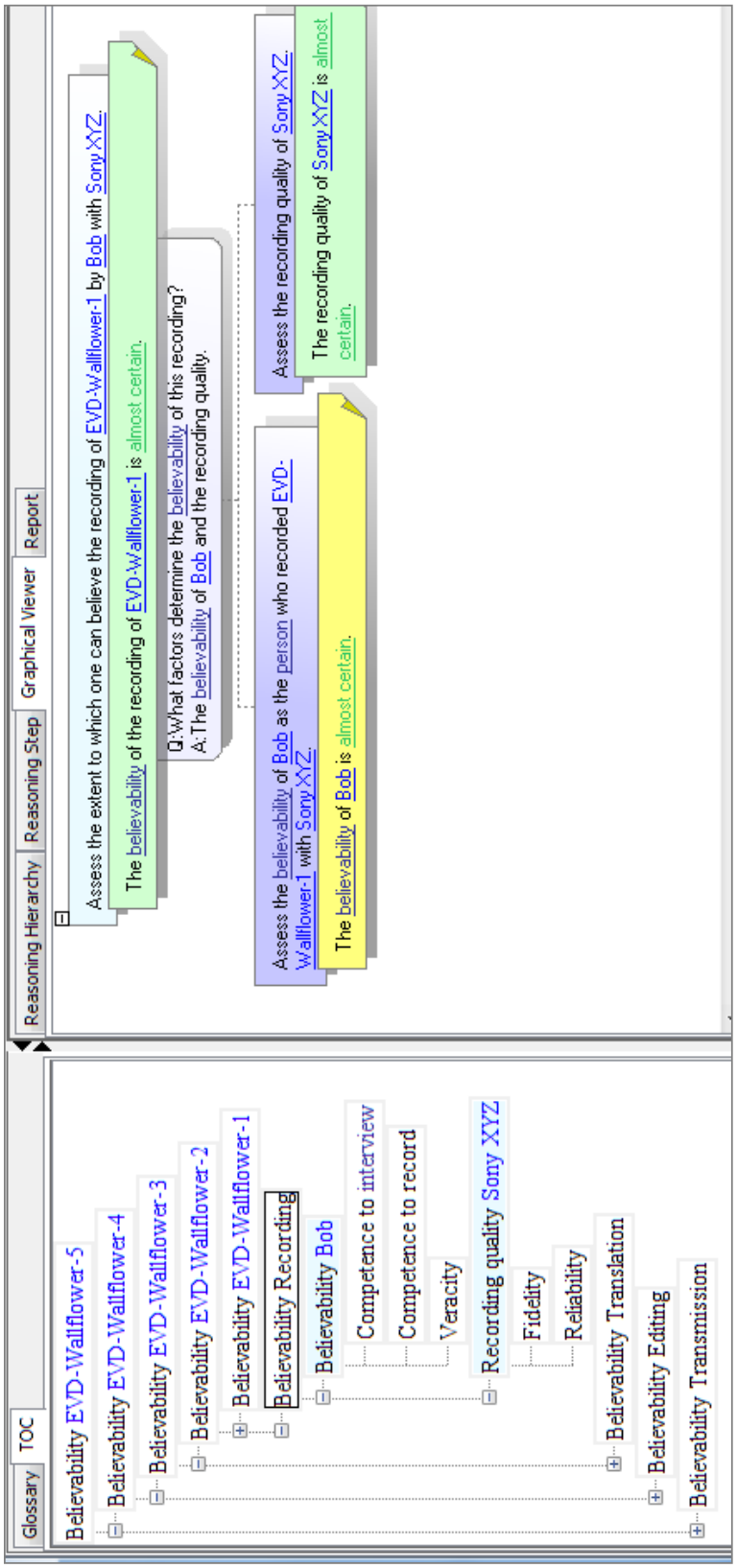

Figure 7: Drill down to analyze the believability of Recording.

When this veracity changed from “almost certain” to “unlikely” (by enabling the assumption from the bottom right of Figure 8), the overall assessment of the believability of EVD-Wallflower-5 changes from “likely” to “unlikely”.

As illustrated above, Disciple-LTA can automatically generate a detailed and rigorous analysis. However, given the astounding complexity of many intelligence analyses, and the often-limited time to complete them, Disciple-LTA also allows the user to perform analytic tasks at several levels of detail; i.e. the analyst can "drill down" to deeper levels depending upon the time available and the evidence necessary to support more detailed levels of analysis. Users are allowed to state various assumptions, to believe "as if", or to "give benefit of doubt" in these situations.

CONCLUSIONS

Much attention has been devoted in Intelligence Analysis to all types of evidence (such as testimonial or tangible), to the ingredients of their believability assessment, and to the employment of specific arguments for such assessments. However, very rarely, if ever, has the analyst access to the original evidence. Most often, what is being analyzed is a piece of evidence that has undergone a serious of transformations through a chain of custody. While there are many possible chains of custody, for different types of evidence (HUMINT, IMINT, MASINT, etc.), they can all be characterized by a chain of basic evidence transformation processes (such as translation, editing, or transmission), as has be illustrated in this paper. Moreover, for each such process, one can identify the ingredients and the arguments of its believability assessment, just as for the different types of the evidence. This paper has introduced and illustrated a systematic, comprehensive approach to the assessment of the believability of all sorts of pieces of evidence and their chains of custody. However, while such a systematic approach would undoubtedly lead to a much better analytic process and much better-founded analytic conclusions, the complexity of the analytic process is so large that all the involved probabilities cannot be assessed. There is simply not enough time for the analyst to assess them or evidence necessary to support these assessments is not available. However, there is a computational solution to this problem, provided by the Disciple-LTA cognitive assistant presented in this paper.

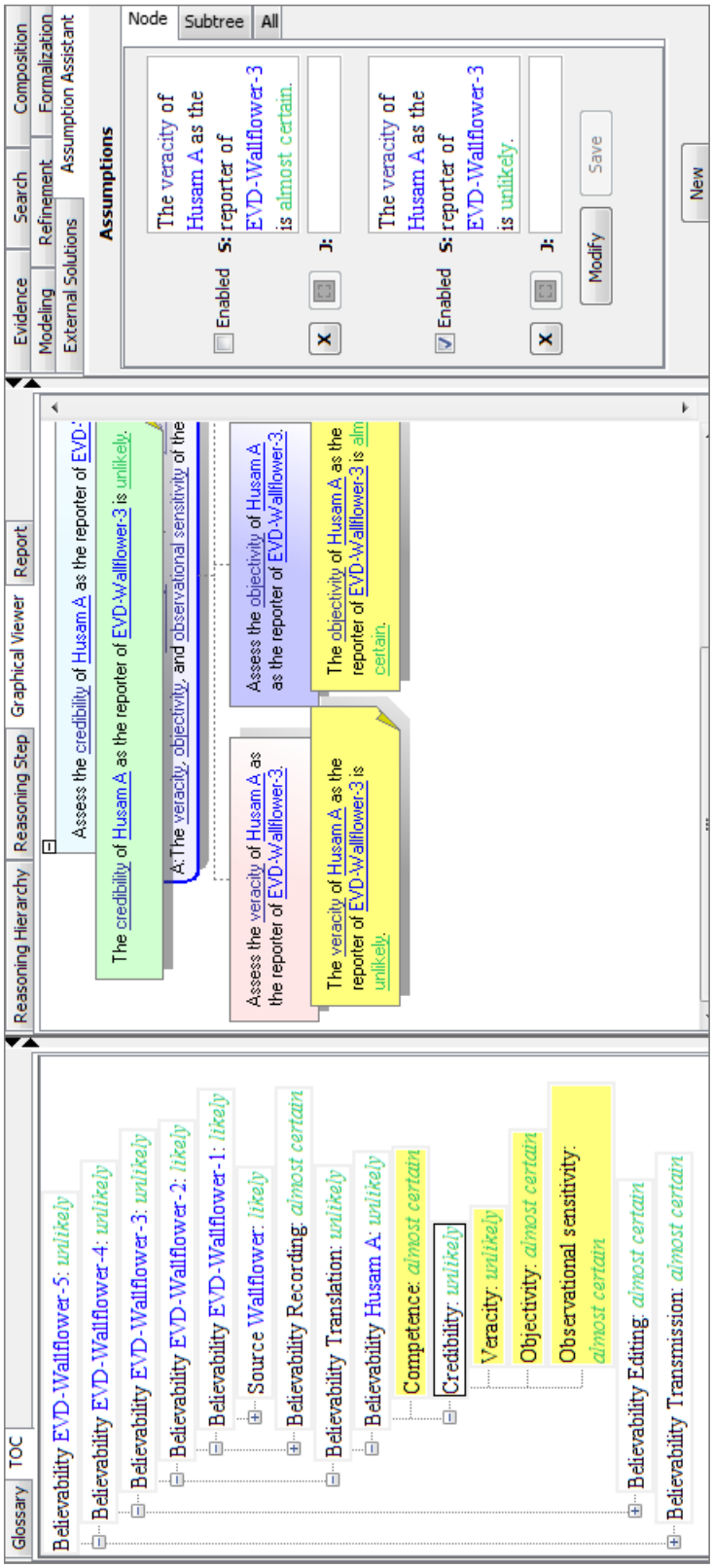

Figure 8: Assumptions-based "what-if" analysis.

Disciple-LTA is a new type of analytic tool that can automatically generate the complex analysis for the analyst, allowing the analyst to drill-down as much as she/he wishes or can, to make assumptions concerning various verbal assessments of uncertainty, and to revise these assumptions in light of new evidence.

ACKNOWLEDGEMENTS

This material is based on research performed in the Learning Agents Center and partially sponsored by several U.S. Government organizations, including the Air Force Office of Scientific Research (FA9550-07-1-0268), the Air Force Research Laboratory (FA8750-04-1-0257), and the National Science Foundation (0750461). The US Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official polices or endorsements, either expressed or implied, of the Air Force Office of Scientific Research, the Air Force Research Laboratory, the National Science Foundation or the U.S. Government.

REFERENCES

Anderson, T., Schum, D.A., Twining, W., *Analysis of Evidence*, 2nd edition, Cambridge, UK: Cambridge University Press, 2005.

Kent S., "Words of Estimated Probability," in Donald P. Steury, (ed.), *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA, Center for the Study of Intelligence), 1994.

Lempert, R.O., Gross, S.R., Liebman, J.S., A Modern Approach to Evidence, 3rd edition, West Publishing Company, 2000.

Nilsson, N.J., *Problem Solving Methods in Artificial Intelligence*, NY: McGraw-Hill, 1971.

Schum, D.A., Inference Networks and the Evaluation of Evidence: Alternative Analyses, *Uncertainty in AI: Proceedings of the Fifteenth Conference*, Morgan Kaufmann, San Mateo, CA, 1999.

Schum, D.A., *The Evidential Foundations of Probabilistic Reasoning*, Northwestern University Press, 2001.

Schum D.A., Lessons and Stories about Concepts Encountered in Disciple-LTA, *Research Report 2*, Learning Agents Center, August 21, 2007.

Tecuci, G., *DISCIPLE: A Theory, Methodology and System for Learning Expert Knowledge*, 197 pages, Thèse de Docteur en Science, University of Paris-South, France, 1988.

Tecuci, G., *BUILDING INTELLIGENT AGENTS: An Apprenticeship Multistrategy Learning Theory, Methodology, Tool and Case Studies*, San Diego, Academic Press, 320 pages, 1998.

Tecuci, G., Boicu, M., Ayers, C., Cammons, D., Personal Cognitive Assistants for Military Intelligence Analysis: Mixed-Initiative Learning, Tutoring, and Problem Solving, *Proceedings of the First International Conference on Intelligence Analysis*, McLean, VA, 2-6 May, 2005.

Tecuci, G., Boicu, M., Marcu, D., Boicu, C., Barbulescu, M., Ayers, C., Cammons, C., Cognitive Assistants for Analysts, *Journal of Intelligence Community Research and Development*, 2007a.

Tecuci, G., Boicu, M., Marcu, D., Le, V., Boicu, C., Disciple-LTA: Learning, Tutoring and Analytic Assistance, submitted to the *Journal of Intelligence Community Research and Development*, 2007b.

Toulmin, S. E., *The Uses of Argument*, Cambridge University Press, 1963.

Weiss, C., Communicating Uncertainty in Intelligence and Other Professions, *International Journal of Intelligence and CounterIntelligence*, 21:1, pp 57-85, 2008.

Wigmore, J.H., *The Science of Judicial Proof*, Little, Brown & Co., Boston, MA, 1937.